SPIRIT STUDIOS.

IT Security Policy

Last reviewed: 11/08/2023

Introduction

Spirit Studios uses a large amount of information in order to operate effectively and the majority of this information is stored in electronic format on computers, servers and cloud services. It is vital that this information remains secure and accessible to authorised users and so this IT Security Policy sets standards for all users outlining the way electronic information and IT systems should be managed and operated.

The IT Security Policy covers all internal Spirit Studios systems, hosted servers, cloud services and connections to wider networks. It sets out how information contained within or accessible via those IT systems should be handled to ensure it remains secure. All systems within Spirit Studios, hosted servers, cloud services and connections to outside bodies must conform to this policy. Spirit Studios reserves the right to isolate any IT system or network which represents a potential or actual breach of security, to monitor information sent over its networks and to deny user access to its IT systems.

This policy applies to all students and staff, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of Spirit Studios.

The Head of Technology has overall responsibility for ensuring Spirit Studios complies with this policy.

Relationships with existing policies

This policy must be read in conjunction with the following policies and guidance applicable to the user:

- Data Protection Policy
- Email Use Policy
- Rules for the Use of IT Facilities
- Student Handbook
- Staff Handbook
- Wireless Network Security & Fair Usage Policy

Monitoring computer usage

Computer usage is logged and Spirit Studios reserves the right to monitor and access any information on the IT facilities, on equipment connected to the IT facilities or on computer media used with the IT facilities for any of the following reasons:

- Record keeping purposes
- Checking compliance with Spirit Studios' regulations and procedures
- Quality control or staff training
- Preventing or detecting crime
- Investigating or detecting the unauthorised use or misuse of the IT facilities
- Checking for viruses
- Reasonably dealing with any other threats or perceived threats to the IT facilities

Traffic Filtering

Spirit Studios filters traffic into and out of its IT network to protect users, systems and information and to help meet its statutory duties. Traffic is filtered for the following reasons:

- To block malicious email, including email transmitting malware or phishing practices
- To reduce spam email
- To prevent external IP-borne attacks
- To prevent access to sites, IP addresses and content that has been prohibited by statutory authorities
- To prevent malicious use of the internet. i.e Distributed Denial of Service (DDoS) attacks on external sites
- To protect users and systems accessing and using known rogue websites

Spirit Studios filters certain internet traffic using policy-based access control, by categories, websites and individual pages. Category filters are set to filter web content which may be deemed illegal or extremist by law enforcement agencies, and for which there is no obvious academic or business requirement at Spirit Studios.

Web sites are categorised and the filters updated frequently via an external service. It is possible that legitimate content may be inadvertently blocked. In such cases a user may appeal in writing (or email) to the Head of Technology for a review of a blocked category or site. The Head of Technology will make the final decision, having consulted as appropriate.

Keeping information secure

Organisational information must be kept secure at all times and be protected from disclosures to unauthorised partners. Personal, confidential or commercially sensitive data must be restricted to those individuals who have a legitimate need for it in order to carry out their responsibilities.

Users of Spirit Studios' IT systems who process personal data must comply with the GDPR legal framework. These requirements are set out in the Data Protection Policy.

Organisational information must only be stored on the Spirit Studios network in shared network drives and databases and in cloud services. Organisational Information must not be stored on portable devices or removable media, such as USB sticks, discs, smartphones etc., or on local PC or laptop hard drives or similar. If users require access to personal data stored on shared network drives when away from Spirit Studios premises, VPN access and Stingray should be used.

Where VPN access and Stingray is not available, temporary storage of information on the types of devices and media outlined above is acceptable provided that the information:

- Is stored on the device/media only for as long as absolutely necessary, and
- Is encrypted (AES Crypt is free to use and available for Windows, Mac and Linux), and

- Is deleted or removed from the device or media as soon as it is no longer required.

For mobile devices (tablets, smartphones etc.), the user must ensure the device PIN or password has been set and that the device is set to automatically lock after a short period of inactivity. This does not replace the need for encryption. Any device without a PIN or password must not be used to hold any organisational information.

Users should never use such devices to store the only copy of information. Should the device be lost or damaged, the information stored on it will not be accessible or retrievable.

Email must not be used for the transfer of personal, confidential or commercially sensitive information unless the information is encrypted. Users must refer to the Email Use Policy when sending personal, confidential or commercially sensitive information by email. Users must not send photographic images of other individuals to external parties obtained from Spirit Studios' email system or any other IT system provided by Spirit Studios.

Computers and other devices must not be accessible to anyone other than authorised users of Spirit Studios' systems. Computers must be locked when unattended to ensure information is not accessed by anyone other than the user who is logged in. Computers must be logged out and shut down after use to maintain security, ensuring all network drives have been unmounted, and to reduce the risk of fire.

Organisational information must not be accessed using VPN access and Stingray from publicly available computers, I.e. Internet Cafes, libraries etc. or a stranger's computer/laptop.

User accounts and passwords

Staff and students will each be given a personal Spirit Studios user account for which they are held responsible. The account is for the sole use of the authorised user to access Spirit Studios' IT facilities. Users must not permit their account to be used by anyone else and users must not use or attempt to use someone else's account.

User passwords must not be shared and be only known to the user. Managers, colleagues and computer system administrators do not need to know a user's

password and must not ask for it. Spirit Studios will not issue any communications that will request you to supply your password. Passwords must not be written down or stored on or near a computer.

Each user account is created with a temporary password. Users must change their password as soon as possible using our self-service password portal. If a user forgets their password, they can use the self-service password portal to reset their password.

Users must follow good security practice when selecting a password. Passwords must be at least eight characters in length and include at least three of the following:

- Upper-case characters
- Lower-case characters
- Numbers
- Symbols

Strings of the same characters should not be used, nor real words or common passwords that would be easy to crack. If users suspect that a password may be known to an unauthorised party, the password must be changed immediately.

Personal computers and external hard drives

Users who are using home computers or other equipment at locations outside of Spirit Studios are operating outside of Spirit Studios' IT security perimeter. In these situations, users must not assume their own computer equipment is protected by the same security measures as computer equipment at Spirit Studios. Weak security on home computers could lead to account passwords being known to unauthorised parties, which could then lead to security incidents involving IT systems at Spirit Studios. The use of external hard drives and other removable media could allow viruses to be transported from unsecured home computers to Spirit Studios. It is vital that computers used for working at home are properly secured and it is the responsibility of the user to do so. This includes:

- Computer, device, operating system and applications are actively supported by the manufacturer (e.g. Microsoft no longer supports Windows 7)
- Up-to-date security patches must be installed for both operating systems and applications

- The computer's local firewall must be enabled
- Anti-virus software is installed and set to automatically update
- Anti-spyware software is installed and set to automatically update
- Wireless networks at home must be properly secured

Users are responsible for safeguarding their equipment against unauthorised access, misuse, theft or loss when in their home or in transit. Users are also responsible for ensuring organisational information is inaccessible by unauthorised parties, including family members.

Phishing, Vishing and Spam

Information security involves technical security measures but also requires users to ensure they act appropriately to maintain the security of computer systems and the IT network. Attacks will be made on these systems and networks by unauthorised parties with the aim of obtaining organisational information, or causing damage or disruption to that information or those systems by infecting them with viruses. Users must be aware of such attachments and be able to recognise them in order to stop them being successful. Attacks may also involve phone calls from individuals trying to obtain confidential information by deception.

Users must ensure that organisational information is only disclosed by phone to callers who are authorised and entitled to receive that information. Further information can be found in the Data Protection Policy.

Users must ensure that they do not click on links in spam or phishing emails. Attachments to such emails must not be opened. Spam and phishing emails are becoming more and more sophisticated and plausible. If in doubt, do not open the mail. Delete it or contact technical support for advice. Users must never email their usernames and passwords in response to emails purporting to be from the technical department. The technical department will never ask for your username and password. If users are in doubt, they should contact technicalsupport@spiritstudios.ac.uk.

Cloud services

Spirit Studios uses cloud services, such as Google Workspace, to store data. Users of such services need to be aware of the following:

- Spirit Studios has no control over the availability of cloud services
- Cloud service providers may carry out periodic updates and maintenance resulting in temporary loss of service for that period
- We utilise Spanning Backup to backup the data in Google Workspace. All individuals can access and restore files from their backups.

Our advice is that if the data is important, another copy should be kept in a secure location (following the guidance of this policy).

IT security incidents

All users must report all actual or suspected security breaches to the technical department (IT Security Incident Form) as soon as they become aware of it, whether they have caused the breach or they have been informed of the breach by another party. The technical department will ensure that any security breaches reported to them are acted upon promptly and will keep appropriate records or documentation. Corrective actions taken and other resolutions will be documented and monitored. In cases where an incident involves personal data, it must also be reported to the Head of Technology without delay.

Back-up and recovery of information

Organisational information in electronic form may only be stored on approved IT services, to ensure it is available for use, backed up and recoverable in the event of an incident. Staff must not store organisational information on individual computers or devices unless exceptional circumstances apply, following advice from the technical department, and Head of Technology where personal data is involved. The system administrators cannot and do not back-up files stored off the shared network drives and cloud services.

Spirit Studios does not accept any responsibility for any student data stored on any workstation or EditShare media space. It is the student's responsibility to ensure they have a secure copy of any data and then a backup of that data at all times. One copy of the data does not constitute a backup. It is highly recommended that students store the data on a USB stick/external hard drives AND on their EditShare media space. Students must check project folders after they have been backed up to confirm all data has been copied successfully.

Loss of projects or data required for an assessment will not be a valid excuse for handing in an assessment late or not at all, and as such students will be marked as late or failed accordingly.

The EditShare server is periodically 'cleaned up', meaning that workspaces no longer required are deleted. This process usually takes place in August but can take place during academic term time if the server runs out of disk space.

Destruction and disposal of equipment

Any equipment or media used to store personal data or other organisational information must be disposed of securely. Users should log a request with the technical department who will refer them to the relevant technician. No equipment or media containing or used to access organisational information must be disposed of or sent for resale without ensuring that all information has been removed and is unrecoverable.

Social networks

Social networks, such as Facebook, Twitter/X and Instagram, are used for official Spirit Studios purposes as well as privately by staff, students and visitors in a personal capacity. Staff and students must not use their Spirit Studios email address for their private social media accounts as it may compromise the security and privacy of Spirit Studios email system and the information it contains.

Copyright

Copyrighted and licensed software must not be duplicated, removed or added to computers by users unless it is explicitly stated that this is acceptable. All copyright requirements must be complied with and declarations must be signed where appropriate.

Spirit Studios' IT systems and network infrastructure, including wireless networks, must not be used for the downloading or streaming of copyrighted materials including, but not limited to, audio and video files, and applications without the written consent of the owners.

Wireless keyboards

Wireless keyboards and input devices are not approved for the general use on Spirit Studios' network as they constitute a potential risk to information security. On this basis, such equipment must not be used. If it is deemed not practical to use an input device connected with a cable, then only wireless input devices using 128-bit encryption are approved.

Similar considerations should be given to the use of wireless input devices at home. Individuals using such devices whilst remotely accessing organisational data must be aware of the risks and take appropriate measures to protect against possible breaches of security.

Use of software

Copyrighted and licensed software may not be copied or distributed by users in contravention of the licensing agreement. Users are not permitted to install or trial software on Spirit Studios systems, nor modify the operating system or any applications in any way.

Personal use of peer-to-peer networking and file sharing applications is not permitted on any of Spirit Studios systems and networks. These applications use Spirit Studios resources for non-learning purposes, they increase the risk of virus infection, increase the risk of spyware infection which compromises privacy and security and they involve legal risks regarding the storage of copyrighted material.

System planning

Proposals for new computers, IT systems or enhancements to existing IT systems must be authorised by the Head of Technology. This is subject to security risk assessments which must be made by suitably qualified staff.

Staff must not contract digital services from external providers without the prior express permission from the Head of Technology. Any external providers who have access to Spirit Studios' organisational information will constitute a data processor under the Data Protection Act 1998 and GDPR legal framework, which

means specific legal obligations must be met. See the Data Protection Policy for further information.