

Email Use Policy

Last reviewed: 11/08/2023

Introduction

Email services are provided to staff, students and other authorised individuals to support Spirit Studios' primary purpose of education and its associated functions. When used properly, email supports efficient and effective processes.

This policy applies to all Spirit Studios staff, students and other authorised users who are provided with a '@spiritstudios.ac.uk' email address, and sets out what is considered to be acceptable and unacceptable use of Spirit Studios' email system. It covers the use of the Spirit Studios email system, including sending, receiving, storing and otherwise processing electronic messages and associated attachments. It also informs users about the management of the email system, the expectations of privacy users of the system should have and helps users and Spirit Studios avoid legal risks which can arise as a result of using email.

This policy may be referred to in the event of disciplinary action arising from or involving use of the email system. Breaches of the policy will be treated seriously and will be subject to sanctions under Spirit Studios' Rules for the use of IT Facilities.

The Head of Technology, with support from the technical department, is responsible for maintaining and updating 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
- IT Security Policy

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

Unacceptable use

Email and related services are provided by Spirit Studios to support its primary purposes of education and their associated functions. Use of the email system is granted to support these primary purposes and must be appropriate at all times. Spirit Studios considers unacceptable use of the email system to include (but is not limited to) email and other electronic messages or attachments created or transmitted (including forwarding) which:

- Bring Spirit Studios into disrepute
- Infringe the copyright of another person or body, including intellectual property rights
- Contain any offensive, obscene or indecent images, data or other material
- Consist of unsolicited commercial or advertising material, chain letters or other junk-mail of any kind
- Are for the purposes of commercial activity or the carrying on of a business which is not related to Spirit Studios
- Inappropriately or unreasonably waste staff and student time, networked resources, or which serve to deny service to other users
- Are intended to cause annoyance, inconvenience or needless anxiety
- Include material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive
- Contain defamatory material
- Contain material which includes claims of a deceptive nature
- By intent or otherwise, harass the recipient
- Violate the privacy of other users or unfairly criticise or misrepresent others
- Are anonymous messages or deliberately forged messages or that have deceptive email header information (i.e. without clear identification of the sender)
- Demonstrate excessive personal use of the system outside of the employee's own time

Research purposes

It is recognised that in the course of their work or research, individuals at Spirit Studios may have a legitimate need to transmit or receive material which would normally be defined as offensive, obscene, indecent or similar. For the purpose of properly supervised and lawful research, it is acceptable to do so if approved in advance by relevant parties e.g. line managers and/or research supervisors and where appropriate ethical approval has been obtained.

Personal use by staff and students

Spirit Studios allows the reasonable use of email for personal use, provided that the level of personal use is not detrimental to the main purposes for which the system is provided. The following guidelines must be adhered to when using Spirit Studios' email system for personal use:

- All personal (non-work) emails must be clearly marked as such in the subject line, to distinguish between personal and business emails
- Personal use of email must not interfere with your work or the work of Spirit Studios
- Priority must be given to the use of resources for the main purposes for which they are provided.
- Personal email must not be for commercial or profit-making purposes or for any other form of personal financial gain
- Personal email must not be of a nature that competes with Spirit Studios in business
- Personal email must not be connected with any use or application which conflicts with an employee's or students obligations to Spirit Studios
- Personal email must not contravene any of Spirit Studios' rules, regulations, policies and procedures
- Users must not forward chain letters, junk mail, jokes and executables
- Users must not send mass mailing
- Users must consider the size of attachments and keep them as small as possible
- Users must remember that all messages distributed by Spirit Studios' email system – even personal emails – are stored by Spirit Studios. Privacy of emails and email content (including attachments) cannot be guaranteed and should not be assumed; emails may be accessed or monitored by the technical department or other staff where there is a legitimate business, employment or other need as outlined in this policy

Monitoring of the email system

Personal (rather than business) emails must be clearly marked as such in the subject line of the emails to distinguish them from each other. Article 8 of the Human Rights Act 1998 (HRA) gives all individuals a right to privacy which extends to the workplace; as such, the content of personal emails sent and received on Spirit Studios' email system will not be accessed unless there is a legitimate need to do so. This right to privacy is not an absolute right; where Spirit Studios can show that there is a legitimate need to access the content of a communication marked 'personal' in our email system and can demonstrate that the resultant invasion of privacy is necessary and proportionate under the circumstances, it can be carried out lawfully in compliance with the HRA.

Email accounts, records and content of emails sent and received by employees, students and authorised users may be accessed (but not necessarily interpreted – see below) by the technical department and management in cases where it is necessary for legitimate business purposes, for the investigation of allegations of improper use or behaviour or to investigate alleged contraventions of any of Spirit Studios' rules, regulations, policies and procedures, where it can be shown to be necessary and proportionate. They may also be accessed for the purposes of crime prevention and detection, the apprehension or prosecution of offenders or for actual or prospective legal proceedings or for the purposes of exercising, establishing or defending legal rights.

In some cases, it may be necessary for Spirit Studios to intercept electronic communications, such as emails. Interception occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. It does not include access to stored emails which have already been opened by the intended recipient. Where interception of communications is deemed necessary and appropriate, Spirit Studios complies with the Regulatory of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR). Under these pieces of legislation, it is lawful to intercept communication if:

- The interception takes place with the consent of the sender and recipient; or
- It is carried out for one or more of the purposes listed in the LBPR, which include:

- Establishing the existence of facts e.g. to provide evidence that a prospective student has been given a specific piece of advice
- Checking that Spirit Studios is complying with regulatory or self-regulatory procedures
- Checking that employees are working to acceptable standards
- Determining whether or not an email is a business communication e.g. checking a person's emails if they are on sick leave or absent for more than a few days to see if any relate to Spirit Studios business and need addressing
- To prevent or detect crime
- To ensure the security of the system and its effective operation
- To investigate or detect unauthorised use of the system e.g. to monitor or investigate compliance with this policy (NB: interception which is targeted at personal communications which are clearly not related to Spirit Studios business purposes is not included and is not made lawful by the LBPR)

Security, data protection and confidential information

Emails are not a secure method of communication. They can go astray, be intercepted, be incorrectly addressed or be forwarded on to a number of people who are not entitled to see them within minutes. If the email is not protected, the information in it or attached to it will be disclosed to people who are not entitled to see it. When sending information by email, users of the email system must take appropriate care to maintain the security and confidentiality of Spirit Studios information.

Users of the email system – particularly employees – are likely to need to send confidential business information or personal data by email on a regular basis. Personal data is any information which relates to and identifies a living individual. It does not have to include their name. The GDPR legal framework requires us to ensure personal information remains secure and is not disclosed to people who are not entitled to see it. Confidential or sensitive business information is any information which relates to Spirit Studios business and has restricted access or is not suitable to be in the public domain.

To maintain security of personal data or confidential business information, it must be sent securely. Sensitive personal data; other personal data which could cause an individual damage or distress if it was inappropriately disclosed; or confidential or sensitive business information must be contained in an encrypted document or folder, which can then be attached to an email and sent

to the recipient. AES Crypt is free to use and is available for Windows, Mac OS X and Linux. Passwords must not be included in the same email as the encrypted attachment and users should ensure that the recipient email address is correct. Users should not email any personal data, confidential or sensitive business information to their own Gmail, Hotmail or other personal (non-Spirit Studios) email account.

Deletion and retention of emails

The email system is not a storage facility. Its primary purpose is for sending and receiving email messages and attachments. If any information contained in an email or attachment needs to be retained as a record of actions, decisions, discussions or information exchanged, it must be moved to an appropriate storage location e.g. a Google Drive or shared network drive, such as Admin (X:) Drive. Folders should be cleared out regularly and information needed as a record saved, as above. Any information which is not required as a record should be deleted. Sent items should also be occasionally deleted, once any emails required as a record have been saved.

When an employee leaves Spirit Studios, any emails which need to be retained for business purposes must be moved to an appropriate storage location.

Staff and student email accounts will be disabled upon exit of Spirit Studios. Staff email accounts are deleted six months after exit and student accounts the first August after exit (for industry students) or fourth August after exit (for academic students). Line managers need to retrieve important emails during an employee's exit procedure.

Deleting emails and the information they contain once they are no longer required saves storage space and reduces costs. Information about the storage space allocated to each user can be found in Appendix B. Storing information contained in emails in an appropriate network location makes it easier to locate and retrieve the information when it is required again in the future and when it is due for destruction.

Third party access to email

Where a member of staff is away from the office for an unexpected or prolonged period of absence which could adversely affect the running of Spirit Studios, the technical department may provide access to an employee's email account for

business purposes. In the first instance, requests for this type of access must be made to the employee's line manager and approved by a senior manager. The technical department will record information about the request and the reasons behind it, the extent and duration of access and who has been given access. As soon as it is practicable and appropriate, the user of the email account must be advised of what has happened. Users granted access to another's inbox under these circumstances must remember that emails which are marked as, or appear to be, private or personal must not be opened or forwarded and must be treated confidentially.

Appendix A: Guidance on appropriate and effective use of emails

Email is an important business tool which is widely used across Spirit Studios. It is important that users understand how to use email appropriately and effectively, to gain the most benefit from the service, protect Spirit Studios from the various risks associated with it and enable staff and students to make the most effective use of their time. Following the guidance below will help ensure this happens:

Writing and sending emails

- Consider whether or not an email is necessary. Another method of communication may be more appropriate in some circumstances e.g. phone call
- Remember that emails are the same as any other form of official communication. They can be taken to represent the views of Spirit Studios when sent from a Spirit Studios email account and should be written with this in mind
- Ensure you use the subject line in every email. Subjects should be brief and meaningful to enable recipients to determine the content of the email and decide if it is something which needs prioritising without necessarily having to read it
- Write well-structured emails, keeping them brief, where possible
- Use the spelling and grammar-checking tool before sending, with the language set to 'English (UK)'
- Do not use smileys/emoticons in business emails
- Do not send unnecessary attachments. Compress large attachments before sending to reduce their size and their impact upon the email system
- Only mark emails as 'high priority', 'urgent' or 'important' if they genuinely are; the impact of using these markings will be reduced if they are used too often and inappropriately
- When sending emails to a group of recipients, consider whether the 'Bcc' facility is more appropriate than the 'To' or 'Cc' facility. This could be the case where you are emailing a group who do not know each other and you need to ensure they can't see each other's email addresses or where

it is not appropriate for each recipient to know who else has received the email

Forwarding and replying to emails

- When forwarding emails, only include recipients who actually need to see the information and ensure you clearly state the action you require each of them to take.
- Consider whether or not it is appropriate to forward an email. Would the sender expect this? Is the content private and/or confidential? Is it commercially sensitive and therefore restricted? Does it contain personal data which should not be further distributed? Ensure you only forward emails when there is a legitimate reason for another person to see the information.
- Reply promptly, even if it is just to explain that you are unable to respond in full at this point but will do so as soon as you are able.
- Consider whether or not it is appropriate to use the 'reply all' function. Do all the people who have been copied into the email you have received need to see your reply? Only reply to those who actually need to see the information in your email.
- Ensure you don't use 'reply all' when you only intended to reply to the sender, particularly for sensitive or confidential emails.
- Particular care should be taken when replying from mobile devices where buttons are more difficult to select.

Checking email accounts

Staff and students should check their email accounts at least once each working day. If this is not possible, an appropriate 'out of office' reply should be turned on, stating when the account will be checked and who can be contacted in the meantime if the email needs urgent attention.

Email Etiquette

- Be aware of how your email may be interpreted by the recipient. Ensure the tone and wording is appropriate and conveys your intended meaning and impression correctly. Email messages can easily be misinterpreted

when there is no vocal intonation or facial expression to support your words

- Do not use email to say something which you would not say to the recipient in person
- Be aware that once you have sent your email, you have little or no control over who else may see it. It can be forwarded on to any number of recipients in a very short space of time. Ensure you only write things which you would be prepared for others to see
- Do not use email to 'get something off your chest' to a large group of people all at once
- Do not copy in members of staff e.g. managers simply to demonstrate that you have done something or asked for a piece of information from someone else, unless they have asked you to. Copying emails to numerous people unnecessarily increases the volume of emails within the system and means recipients who may not need to see an email must spend time reading them, potentially for no reason

Appendix B: Quotas and limits

- Attachment size limit (sending): 25 MB
- Attachment size limit (receiving): 50 MB
- Recipients per message (To, Cc, Bcc fields combined): 2000 (500 external)
- Unique recipients per day: 3000 (2000 external)