# AUP: Email Policy

## Purpose

This document addresses the risk of using email, the policies required to manage those risks to an acceptable level and the responsibilities within the business to achieve this

## Introduction

Security Policy is an essential measure to help protect Rose Bruford College information systems from compromise, either accidentally or deliberately, which could have an adverse consequence on the college, its management and staff and students. This document addresses the risk of using email, the policies required to manage those risks to an acceptable level and the responsibilities within the business to achieve this

## The structure of this document is described in the table below.

| Section | Description |
|---|---|
| Background to Risk | Examples of email risks including recently publicised cases |
| The User Policy | Describes the policies that all email users must follow |
| Management Responsibilities | Describes management's role in supporting the policy |
| Technical Support Responsibilities | Describes IT role in supporting the policy |

Related policies include:

- Standards and Guidelines for all users of College Computing and Network Facilities
- Internet Acceptable Use
- Virus Protection Policy
- Data Protection and Monitoring
- Password
- Personnel Security

## Background to Risks

Email is part of the lifeblood of Rose Bruford College, but accidental or deliberate misuse can have a number of serious impacts upon the college. Here are several potential risks with examples using cases that have been publicised:

**Risk - incorrect Business Use by Staff or Student**
With click of mouse employee can accidentally send an email either internally or externally to the organisation that results in embarrassment to management, discloses confidential information to the wrong recipient, or results in an unauthorised contractual commitment. A libellous email can also be used as part of incriminating evidence during legal proceedings against the organisation by an employee, or by an external party. The impacts to the college could include settlement or court fines, loss of customers or potential clients or damage to public reputation.

**Risk - Inappropriate Personal Use by Staff or Student**
An email that was of a personal but sensitive nature was forwarded to other member of staff or student, and external email addresses. For example, a distasteful joke or remark about someone sent is to a friend, which is subsequently forwarded to journalists and is published. The college's reputation could be severely damaged – depending on type of business and contents of email.

**Risk - Offensive Content from Staff, Students or Outsiders**
Distribution of porn or otherwise offensive content can affect the moral of staff, result in serious embarrassment to the college and its management with potential loss of students and damaged reputation. The college could be embroiled in lengthy and costly legal cases which also use up staff and management resources.

**Risk - Chain Emails, Hoaxes, SPAM and forged emails**
Chains and Unsolicited emails (e.g. SPAM) affect staff and students productivity, can be annoying and affect the operation of email services and network resources. Emails with large attachments such as images or video clips also impact the operation of the email service.
Up to 65% of emails are SPAM and significant resources are spent by ICT staff dealing with this on a daily basis. Forged emails can lead a member of staff or student carrying out an activity that could disclose confidential information or otherwise jeopardise the college. Email scams can result in impact to staff and student productivity, and scams directly targeted at certain types of business could lead to disclosure or other types of losses by students or members of its staff.

**Risk - Corruption by Malicious Content**
Email continues to be one of the main sources for the transfer of malicious software around the Internet, affecting the availability and integrity of workstations and severs. Email worms may contain or cause the download of software that results in Distributed Denial of Service (DDoS) attacks against other Internet websites, or otherwise uses the resources of one company's information systems to launch attacks on another. The college reputation would be badly damaged by such an incident; the organisation could be sued and may have to pay for remedial work to its own systems.

**Risk - Use of Personal Email Systems**
College email that is created on, forwarded to or otherwise stored on email systems outside of the college's control will be bypassing many of the controls implemented to meet the email policy requirements, including email disclaimer statements, and cannot be monitored by the college.

**Risk - Copyright Infringement**
Software executables that are distributed via email either into or out of Rose Bruford College may result in an infringement of copyright rules. This could result in embarrassment to Rose Bruford College and large fines.

## Management Responsibilities

In relation to email, the college Principal is responsible for ensuring the college's compliance with all current legislation and corporate governance. The Principal has a responsibility to governors, students and staff to safeguard college assets and viability and for preserving the college's integrity and reputation.

Management are responsible for:

- Implementing this email policy, monitoring its effectiveness, maintaining it
- Ensuring that staff and students are made aware of policy contents and confirm their understanding by appropriate means
- Handling individual exceptions to rules, e.g. for business or technical reasons
- Adhering to the User Policy principles and thereby showing the correct example
- Ensuring that breaches of policy are treated even-handedly no matter the level of staff involved
- Discipline will be applied as defined in the Student Handbook / Staff Handbook
- Ensuring that any requests by an individual to gain access to another's email account, e.g. on extended leave or sickness is approved and documented

The effectiveness of the policy will be monitored by carrying out the following activities:

- Formal information security awareness / training
- Reviewing content management reports
- Gaining feedback from email users
- Monitoring content in accordance with the UK Privacy Directive – i.e. if it is justified and there has deemed to be a breach of security

## User Responsibilities

The following two sections detail the user email policy principles at Rose Bruford College that must be followed by all users. In the event that users are not clear of any policy principles they should seek clarification from the Head of IT.

These are the essential principles of the email security policy which must be followed by all email users, whether, employees or directors:

- Email facilities are intended for business use. A limited amount of personal use is allowed subject to management agreement;
- All college emails sent to external email addresses will have a corporate signature added (see below for template);
- The college corporate email signature template (see below) must not be altered or removed on any external email communication;
- Emails which may be considered libellous, or otherwise detrimental to Rose Bruford College, must not be transmitted internally or externally to the organisation;
- Emails which are offensive in e.g. a racial, sexual, religious, ethnic, or any other nature are not permitted to be transmitted using email;
- Unsolicited emails such as Spam should be deleted and must not be passed on to other internal or external email addresses;
- Emails that are clearly not business related and are in any way suspicious, e.g. "meaningless" sender, subject or attachment name must be deleted;
- Emails that are of a "phishing" nature or scams that are unsolicited but prompting for any sensitive information such as credit card details, PINS, passwords by way of a hyperlink to a site that even appears authentic must not be opened, or forwarded and should be deleted (some legitimate emails may contain links to a site logon page, for example as a result of the user selecting the "forgotten password" link on a legitimate website;
- Staff and students should not create, store or automatically forward college emails to an outside email address;
- The authenticity of an external email origin as stated in the email header must not be relied upon, in particular for requests for information;
- Users are accountable for usage of their own email accounts and must not share their own password with other individuals;
- Users should not send confidential or highly sensitive personal information externally without using additional security measures such as encryption;
- Failure to comply with any of the above policies principles may result in disciplinary action.

## Policy for avoiding errors

The following principles should be adhered to by users to maximise the effectiveness of the email systems and to reduce the risk of accidental error. Email users should:

- Avoid sending large attachments without compressing them first, and should not send large attachments at all for personal use. Personal email recipients should be advised not to send these attachments into the organisation
- Be careful with the tone and etiquette of emails
- Be careful with addressing emails, use of read receipts requests for acknowledgements and care when using "reply all"
- Ensuring that Mailing lists clearly identify if any members are external to Rose Bruford College

- Be careful when addressing emails using mailing lists to ensure that emails are not sent inadvertently to external email addresses

To help ensure that user privacy is maintained, personal emails (subject to the limitations described) should be marked “personal” as advised by the Data Protection Code Part 3.

## Monitoring of User Emails

The college reserves the right to intercept, read and store any email on its systems or in transmission over its network in the UK at its discretion. All interceptions will be carried out in accordance with current legislation.

## IT Support Responsibilities

The IT personnel supporting the email service have the following responsibilities:

- Complying with the policy principles as users
- Creating unique email accounts for individuals only. Generic or shared accounts must only be created if justified by college or technical requirements, must be approved by management and documented
- Giving access to email accounts, resetting passwords in line with separate policy. Access in event of absence to be extended by permissions if possible in preference to divulging passwords
- Removing the ability to logon to email accounts once users have left the organisation
- Ensuring that agreed email disclaimer is applied to all outgoing email messages
- Ensuring that all incoming and outgoing emails are virus checked (refer Virus and Content policy)
- Ensuring that backups of emails are stored securely and that archives are retained as specified
- To ensure that email are destroyed after the agreed retention period
- Ensuring that access to internally stored mailing lists from outside of the college are controlled, justified and approved
- Making sure that IT support staff are familiar with the relevant Privacy Directive legislation and do not read personal email (so marked)
- The monitoring of communications by unauthorised individuals is prohibited and may be illegal. Interception and monitoring may only take place with explicit written authority and must be justified and fully documented

NOTE
Data Protection Code Part 3 recommends that only sender and recipient name and subject are monitored.

**Disclaimer Text - Staff**


**Disclaimer Text - Students**

**Ellie Sambrook**
**Student : 1304432**
**BA(Hons) Stage Management**

Rose Bruford College
Lamorbey Park Campus
Burnt Oak Lane
Sidcup
Kent. DA15 9DF. UK
Tel: +44(0)20 8308 2600  Fax: +44(0)20 8308 0542