Dev Sanskriti Vishwavidyalaya – Email & Social Media Policy

(Version 1.0)

Controlled Document – Must not be copied in whole or in parts by any means without the written authorization of Chancellor, Vice Chancellor / Pro Vice Chancellor of Dev Sanskriti Vishwavidyalaya.

Document Release Notice

This leave policy document is released for use in Dev Sanskriti Vishwavidyalaya (DSVV) with effect from <DD-MMM-YYYY> and is subject to DSVV Document Control Procedure.

Approved By:

Authorized By:

Document Version Control

Revision / version No.	Effective Date	Document Release/Revision Date	Revision Description	Section	Rationale for Change	Change Type (Add/Modify/Delete)	Document Process/Policy Revision
1.0	30-Dec-2020	30-Dec-2020	First Release	NA	NA	NA	NA

Contents

Email

Introduction

Email and other forms of electronic messaging are important and much-used services within DSVV. Email and messaging services are provided by the University to support its primary purposes of education and research and their associated functions. When used properly, email and other electronic messaging supports efficient and effective business processes.

This policy sets out what is considered to be acceptable and unacceptable use of the University's Email System. It informs staff about the management of the Email System; the expectations of privacy users of the system should have and helps users and the University avoid legal risks which can arise as a result of using email and other types of electronic messaging.

In this policy, Email System means the email system itself and any other IT products, technology and facilities which the University makes available for the purposes of sending or receiving electronic messages and attachments, instant messages (e.g. via Skype or Teams) and other similar communications including those sent via social media. Email is used to refer to emails and other types of electronic messages.

Note: - Users should use their own password protected accounts for email communications.

Scope

The policy applies to all University staff, students, vendors, partners and other authorized users who are provided with an '@dsvv.ac.in' domain email address or provided with access to other electronic messaging facilities provided by DSVV. It covers the use of the DSVV Email System, including sending, receiving, storing and otherwise processing electronic messages and associated attachments. It may be referred to in the event of staff or student disciplinary action arising from or involving use of the Email System. Breaches of the policy will be treated seriously by DSVV and will be subject to sanctions under the University's Rules for the Use of IT Facilities.

Unacceptable use

Email and related services are provided by the University to support its primary purposes of education and research and their associated functions. Use of the Email System is granted to support these primary purposes and must be appropriate at all times. DSVV 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 the University 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 DSVV or AWGP
- inappropriately or unreasonably waste staff time or 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, pedophilic 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 others or unfairly criticize 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
- Intentionally spam other people's emails, including their coworkers

Research Purpose

It is recognized that in the course of their work or research, individuals at the University 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

DSVV does not allow the reasonable use of email and other electronic messaging for personal use, except for special scenarios. Users will adhere to the following guidelines when using DSVV's Email System for personal use:

- All personal (non-work) emails must be clearly marked as such in the subject line as #Personal#, to distinguish between personal and business emails
- Personal use of email must not interfere with your work or the work of the University
- Priority must be given to 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 the University in business
- Personal email must not be connected with any use or application which conflicts with an employee's obligations to the University as his or her employer
- Personal email must not contravene any of the University's rules, regulations, policies and procedures

- Users must not forward chain letters, junk mail, jokes and executables
- Users must consider the size of attachments and keep them as small as possible
- Users can Register for classes or meetups from official email which is for academic purposes only
- Can give their email address to people they meet at conferences, career fairs or other corporate events for business purposes
- Can sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth
- Copyrighted materials belonging to entities other than DSVV should not be transmitted by users on the company's network without permission of the copyright holder.

Users must remember that all messages distributed via DSVV's email system - even personal emails – are stored within the DSVV's Email System. Privacy of emails and email content (including attachments) cannot be guaranteed and should not be assumed; emails may be accessed or monitored by IS or other authorized staff in cases where there is a legitimate business, employment or other need.

Monitoring of Email

Users will clearly mark #personal# (rather than business) emails as such in the subject line of the emails to distinguish them from each other. Human Rights Act gives all individuals a right to privacy which extends to the workplace; as such, the content of personal emails sent and received on the DSVV system will not be accessed unless there is a legitimate need to do so. This right to privacy is not an absolute right; where the University 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 may be accessed (but not necessarily intercepted – see below) by IS, HR and managers in cases where it is necessary for legitimate business purposes, for the investigation of allegations of improper use or behavior or to investigate alleged contraventions of any of the University's 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 the University 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, the University complies with the Regulation of

Information Technology Act, Indian Telegraph Act and IT amendment Act. Under these pieces of legislation, it is lawful to intercept communications if-

- the interception takes place with consent of the sender and recipient; or
- it is carried out for one or more of the purposes listed below, which include
    - establishing the existence of facts e.g. to provide evidence that a customer has been given a specific piece of advice
    - checking that the University 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 University business and need addressing
    - to prevent or detect crime
    - to ensure the security of the system and its effective operation
    - to investigate or detect unauthorized 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 DSVV business purposes is not included and is not made lawful by the LBPR).

Security, Data Protection & Confidential Information

When sending information by email, users of the Email System will take appropriate care to maintain the security and confidentiality of DSVV's 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. Data protection legislation requires DSVV to ensure that 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 DSVV 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. Special category personal data; other personal data which could cause an individual damage or distress if it was inappropriately disclosed; or confidential or sensitive business information will be contained in an encrypted document or folder, which will then be attached to an email and sent to the recipient. Passwords will not be included in the same email as the encrypted attachment and users will ensure that the recipient email address is correct. With the exception of students sending their own personal data to their own email accounts, users will not email any personal data, confidential or sensitive business information to their own Gmail or other personal (non-DSVV) email account. Personal, non-DSVV email accounts will not be used for DSVV business and business data will not be sent or copied to personal email accounts.

Email Retention

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 will be moved by the user to an appropriate network location e.g. a shared network drive or SharePoint then deleted from the inbox. DSVV's Retention Schedule provides direction about how long certain classes of information should be retained.

When it is due for destruction. Users will be made aware that any information they keep (whether or not it is required by the University) can be requested under data protection legislation or IT Amendment Act and may have to be disclosed to the person the information is about (if it is personal data) or into the public domain. This includes information and discussions contained in or attached to emails.

Out of Office and Delegation

When a member of staff is away from the office for planned period of vacation could adversely affect the running of the University, DSVV may provide access to an group email account for business purposes to multiple users.

It is advisable to have out of office message for time off days with a clear mention of duration of time off and an alternate contact in the message, to which the sender of the email can contact for any urgency.

Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every two months.
- Also, users should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:
    - Avoid opening attachments and clicking on links when content is not adequately explained
    - Be suspicious of clickable titles.
    - Check email and names of unknown senders to ensure they are legitimate.
    - Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

- If an employee isn't sure that an email they received is safe, they can ask our Security Specialists

Email signature

We encourage users to create an email signature that exudes professionalism and represents our organization well. Executives, who represent our company to customers and stakeholders, should pay special attention to how they close emails. Here's a template of an acceptable email signature:

[Senders Name]

[Title], [Company Name with link]

[Phone number] | [Company Address]

Employees may also include professional images, DSVV logos and work-related videos and links in email signatures. If they are unsure how to do so, they can ask for help from IS team or their supervisor.

Confidentiality Disclaimer

Kindly include the below message for sending email outside he organization at the bottom of email.

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

Viruses & Phishing

Emails can pose a security risk to your business. They are often used to distribute viruses and spyware, or for phishing attempts.

Our email service provided by Google includes protection to reduce risks. However, even the strongest filters will allow the occasional malicious email to slip through.

Kindly take care of following points

1. Delete attachments from unknown sender
2. Take care while downloading or opening file types with extensions - .vbs, .js, .exe, .bat, .cmd or .lnk
3. Kindly inform the IS team if you receive a suspicious attachment of if you suspect a virus has entered in to the system.

Mass Email Communication

Introduction

DSVV aims to empower its staff members with critical information at right time through the right communication channels. With the rising needs to disseminate information to multiple stakeholders at the same time, internal communications through email broadcasts are widely increasing. In order to communicate effectively and maximize assimilation of information by staff members DSVV had laid down guide lines for mass email communication.

DSVV encourages the authorized personnel to leverage on mass emails only for the purpose of broadcasting essential and time sensitive information relevant to targeted and large groups.

Communication is considered as essential if any of the below criteria is met –

- It is mission critical and pertains to business continuity / emergency situations
- It is required by law
- It outlines key organizational changes, announcements, promotes processes and protocols to be followed or is pertinent to employee capability building and growth.
- It pertains to employee health and wellness

Creative Guidelines

1. The content in email is required o be brief, self explanatory, concise and must comprise of minimal text. If additional information is required to be shared with the recipients, the authorized personnel are expected either to link the email to an internal URL / path or seek alternate communication channel.
2. An upper limit of 60 characters for the title of the content and that of 300 words for the email content is advised to be maintained.
3. The specifications for formatting are as follows
    a. Aerial, Sans serif or serif font should be used for entire creative
    b. All heading are expected to be maintained within a font sixe of 22 to 25
    c. All body text is expected to be maintained within a font size of 6 to 20
    d. The authorized personnel is expected to use the palette colors approved by DSVV branding team only and refrain from using dark / varied colors.
    e. A maximum o three colors can be used for the creative.
4. A concise and relevant subject line of up to maximum 50 characters, conveying the email purpose must be included.
5. The permissible size limit for the entire email along with any attachments is up to 1MB. It is advised to provide an internal link / path or contact details in the email from where recipients may obtain more information.
6. The overall limit for broadcast emails across DSVV should be 5 per day.

7. Any critical and time sensitive messages pertaining to leadership communication shall take precedence over other email requests.
8. Prior to being considered for deployment, the email content is required to be authorized by ERP / HR/ Accounts or Pro VC office based on content.
9. The authorized personnel is expected to use their group communication id for the purpose of broadcasting.

Social Media

Applicability & Scope

This policy applies to both external and internal social media networks. Through this policy, DSVV endeavors to –

- Encourage the use of social media for individual and business benefit.
- Empower the staff members to be aligned with corporate vision and goals and create a high performing and innovative organization.
- Optimally leverage social media as a means to conduct our working or business.
- Increase interconnectivity and foster a collaborative environment to exchange ideas.

Appropriate usage

- While using social media, users shall comply with all applicable laws including but not limited to laws governing intellectual property rights, data protection and financial disclosure regulations.
- Issues arising out of an individual participation in social media shall be the responsibility of the participant and DSVV shall not be held liable in any way for such issues.
- Information published by DSVV authorized users on social media should not be taken as conclusive ad acted upon before receiving a written confirmation on the same from DSVV
- Individual participants in social media shall not use DSVV branding – logos, trademarks, visual identity – on their blog, profile or group page. Only DSVV owned blogs, company profiles and DSVV administered groups may use the DSVV brand identity.
- Online harassment of any form shall not be tolerated. This can compromise of, but not limited to practices such as sending inappropriate, harmful, explicit or threatening messages to known and unknown individuals in public or private. E.g. Facebook messenger, twitter etc.
- Terms and conditions laid down by any social media platforms should be followed in its entirely.
- One t one discussion on social media should be done with caution and care.
- Sharing of audio or video footage on personal social media networks should not include DSVV logo or any DSVV confidential information.
- Special attention and care should be used before sharing one's own or others personal information. Sharing of others personal information should strongly be discouraged. Using or

sharing of others personal information should be done only when permitted by concerned individual or when it is allowed by local law.

Social Media Publication Authorization

- External social media –Chancellor's office or Office of Pro Vice Chancellor
- Internal Networks – HR, HOD, Registrar's office, Office of Pro Vice Chancellor, Chancellor's Office

While using external social media, users shall disclose their identity with complete contact details including an active email id and telephone numbers or provide a link to the page that has such information.

Individuals can express their opinions on the network. However DSVV will not be responsible for any statement or opinion posted by an individual user.

Monitoring

DSVV reserves the right to monitor contents, comments or discussions about itself or its staff and the industry including products and competitors, posted by the users on social media. DSVV reserves the right to seek clarification on any content posted on social media by users at any point of time and also block or delete content that conflicts with DSVV values or any other policies or procedures.

Making of derogatory comments on social media which is or is likely to insult or insinuate any individual or community on basis of religion, ethnicity, language, race, gender etc is strictly prohibited. DSVV reserves the right to remove / delete such opinions from its social platforms. DSVV reserves the right to take strict disciplinary action against the concerned employee based on the severity of the views expressed.

Reporting violations & Disciplinary actions

Violations can be reported in writing to Office of Pro Vice Chancellor.

Disciplinary action may range from a warning to termination of employment.

General Guidelines

- Use care while communicating with minorities
- Do not start arguments or fuel them
- Be the first to respond to your own mistakes
- Use your best judgment
- Direct official enquiries to right authority
- Protect your clients and suppliers
- Respect your audience and coworkers
- Take ownership and responsibility

- Do not share information that isn't meant for public disclosure
- Don't post anything when in doubt
- Do not post inaccurate or unverified information
- Do not create pages or handles on behalf of organization without explicit permission
- Do not borrow or steal content originally published by others to pass it off as yours
- Don't let social media interfere with your responsibilities
- Don't forget that everything that is posted on internet is permanent
- Don't embarrass yourself or organization

Internet Usage

This internet usage policy is intended to provide guidelines for the acceptable use of the internet used in connection with DSVV**.** The guidelines set in this policy are intended to provide examples of inappropriate behaviors that are prohibited in DSVV**.**

This policy applies to all employees, contractors, and other associates of DSVV**.**

Unacceptable ways of using internet at workplace

- Distributing harassing, violent, discriminating or hateful messages and imagery by the means of company equipment;
- Utilizing the Internet and computers at the working place in order to commit any kind of illegal activity, including piracy of music, movies, and other content;
- Appropriating someone's login information and using it without permission;
- Illegally downloading, managing or uploading copyrighted content via the company computers;
- Distributing secret company information outside the company;
- Posting derogatory information regarding the company, its owners or other employees;
- Installing inappropriate software that could be harmful to the equipment and network at the working place;
- Distributing spam emails and posts via the company equipment and the Internet;
- Posting information based on your personal beliefs and presenting it as those shared by the whole company.

Piracy, data theft, hacking, and other illicit or unsafe activity

The following activities are strictly forbidden on company equipment:

- Illegally downloading music, films, software, and other digital goods ("Piracy")
- Installing software on company computers without the authorization of a company information technology (IT) representative
- Sharing confidential material, trade secrets, or other proprietary information outside of authorized parties of DSVV
- Gaining unauthorized access to programs, systems, websites, etc ("Hacking")

- Introducing malicious software ("Malware") onto the company network or performing other actions that put the security of the organization at risk
- Attempting to bypass the company web filter to access blocked material
- Accessing content that would reasonably be considered not safe for work such as pornography, violent imagery, and other adult-oriented content.
- Sharing or leaking passwords or other credentials that are used to provide access to company equipment, services, accounts, and other company assets.

Employee monitoring

The equipment used to access the internet is the property of DSVV. DSVV may use employee monitoring software to ensure the acceptable use of technology by employees, maintain the security of company data and property, and assist with employee productivity tracking. This activity tracking software will be used to monitor employee computer activity, including monitoring internet activity such as the websites visited by employees.

Copyrights

All data that is created on DSVV computer systems is considered to be owned by DSVV**.** Unauthorized disclosure of this data is not permitted and DSVV reserves the right to disclose this data to authorized parties at its discretion.

Disciplinary action

Those found to be in violation of this policy may be subject to corrective measures up to and including termination of their employment with DSVV

Amendments to this policy

The terms of this policy are subject to change at the discretion of DSVV**.** New updates will be available in the DSVV portal.