THE UNIVERSITY OF BRITISH COLUMBIA Facilities	**Policy No.:** **I-A-P4**	**Approval Date:** May 27, 2021 **Last Revision:** April 2020 Previous Policy P31
	Responsible Executive: John Metras Associate Vice-President, Facilities	
	Signed: John Metras	

Title:

FACILITIES COMMUNICATIONS POLICY

Background & Purposes:

The purpose of this policy is to ensure the proper use of UBC Facilities communications systems and to make users aware of what Facilities deems as acceptable and unacceptable use. Facilities reserves the right to amend this policy at its discretion. In case of amendments, users will be informed.

Facilities Communications are governed by UBC Policy SC14 on Acceptable Use and Security of UBC Electronic Information and Systems, which can be located here: http://universitycounsel-2015.sites.olt.ubc.ca/files/2019/08/Information-Systems-Policy_SC14.pdf

UBC Information Security Policy, Standards & Resources are also to be reviewed and are located here: https://cio.ubc.ca/information-security/information-security-policy-standards-and-resources#user_standards

1. Mobile Devices and Smartphones

1.1. Smart devices provided by the department are UBC electronic systems and are governed by the Information Systems Policy SC14. Review this policy to be sure you are aware of your responsibilities with respect to the acceptable use and security of University electronic information and the services, devices and facilities that store or transmit this information.

Mobile Device User Responsibilities:

- Mobile devices are to be used in a manner which is consistent with the Safety, Security, and Appropriate Use policies of the University mentioned above. Employees must familiarize themselves with UBC Policy SC14 and the UBC Information Security Policy prior to using a mobile device.

- Appropriate and respectful language is to be used during all forms of communication on mobile devices. No communication is to contain any libelous, defamatory, offensive, racist or obscene references or remarks.

- Employees must make efforts not to use UBC mobile devices to permanently store UBC data, and should use UBC-Approved storage systems if long-term storage of information is required.

- Employees must refrain from storing personal use records on any UBC mobile device, including credit card information, photos, personal text messages and other records as defined by UBC Policy SC14, to prevent unintentional loss or exposure of personal information.

- Employees must keep managed device passcodes private, not storing them visibly, either on the device or in other obvious locations.

- Mobile devices assigned by UBC remain the property of UBC

1.2. As per Facilities policy I-C-07 section 4.3.1, staff are not to use any hand held electronic devices while driving as per 30.07 of the motor vehicle act.

1.3. For a full review of appropriate use guidelines, refer to UBC IT Policy – Appropriate Use
https://it.ubc.ca/services/email-voice-internet/resnet/appropriate-use

2. E-mail Communication

Facilities considers email and other electronic communications important means of communication. Proper email and electronic communication content and timely replies are important in maintaining a professional environment and delivering excellent customer service. Messages sent and received through UBC information systems are governed by the **UBC Information Systems Policy SC14.** Facilities urges users to adhere to the following guidelines:

2.1. Do not use personal email account for work purposes. Refer to Privacy Matters Use of Personal Email Accounts.

2.2. Communication through email messages must be done in a responsible and professional manner.

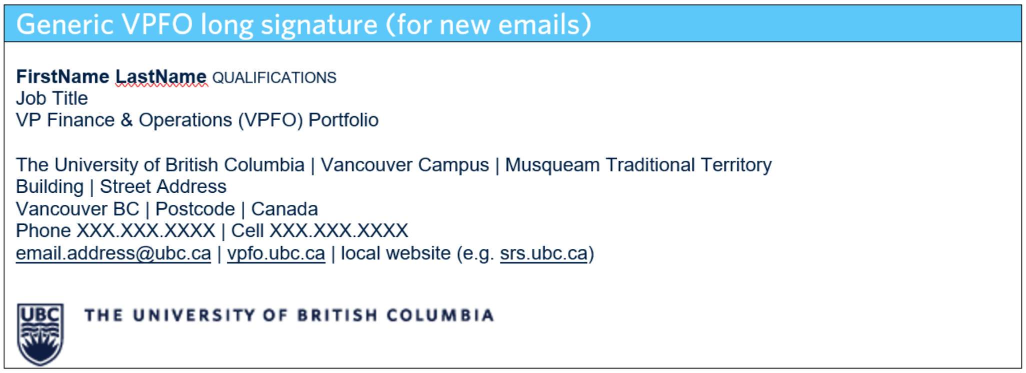
2.3. Signatures must only include your pertinent contact information. Use only UBC Brand approved logos, images and icons. Visit https://communications.vpfo.ubc.ca/produce/tools/templates/ for guidance and to generate email signature.

Signatures must have:

- VP Portfolio:
- AVP Group:
- Department:
- Division:
- Unit
- Teams (optional)

For example:

- VP Portfolio: VP Finance & Operations
- AVP Group: Facilities
- Department: Building Operations
- Division: Trades
- Unit: Sheet Metal
- Teams (optional) Special Projects

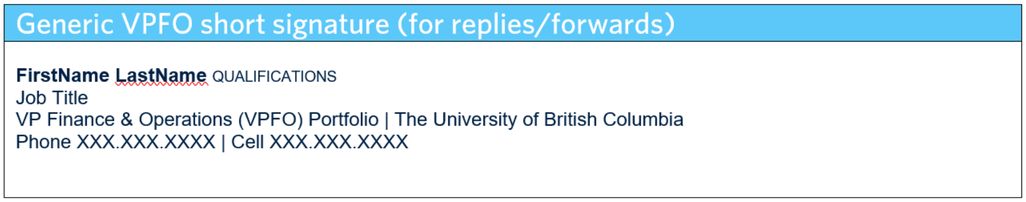


Generic VPFO long signature (for new emails)

FirstName LastName QUALIFICATIONS
Job Title
VP Finance & Operations (VPFO) Portfolio

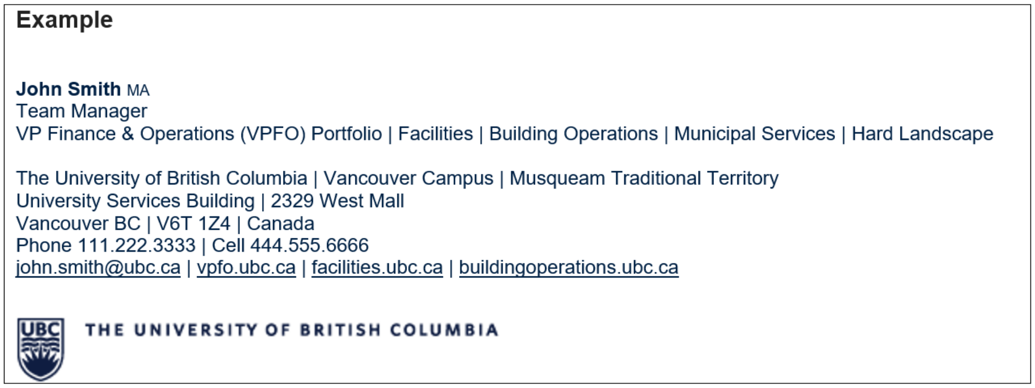
The University of British Columbia | Vancouver Campus | Musqueam Traditional Territory
Building | Street Address
Vancouver BC | Postcode | Canada
Phone XXX.XXX.XXXX | Cell XXX.XXX.XXXX
email.address@ubc.ca | vpfo.ubc.ca | local website (e.g. srs.ubc.ca)

UBC THE UNIVERSITY OF BRITISH COLUMBIA



Generic VPFO short signature (for replies/forwards)

FirstName LastName QUALIFICATIONS
Job Title
VP Finance & Operations (VPFO) Portfolio | The University of British Columbia
Phone XXX.XXX.XXXX | Cell XXX.XXX.XXXX



Example

John Smith MA
Team Manager
VP Finance & Operations (VPFO) Portfolio | Facilities | Building Operations | Municipal Services | Hard Landscape

The University of British Columbia | Vancouver Campus | Musqueam Traditional Territory
University Services Building | 2329 West Mall
Vancouver BC | V6T 1Z4 | Canada
Phone 111.222.3333 | Cell 444.555.6666
john.smith@ubc.ca | vpfo.ubc.ca | facilities.ubc.ca | buildingoperations.ubc.ca

UBC THE UNIVERSITY OF BRITISH COLUMBIA

Email Security and Best Practices:

Email is a business communication tool and users are obliged to use this tool in a responsible, professional and lawful manner. Although by its nature email can appear to be less formal than other written communication, it should be treated as any other formal communication tool and it is important that users follow all guidelines listed below when using e-mail to minimize potential risks. Failure to follow these guidelines could create legal liability for UBC and, in some cases, could lead to discipline or personal liability for yourself.

- Do not send or forward emails with any libelous, defamatory, offensive, racist or obscene remarks.

- Do not use email to send large amounts of confidential information. Instead use a secure data sharing tool such as UBC OneDrive.

- Do not forward or copy messages containing non-UBC copyrighted material without permission.

- If you receive a spam or phishing email (learn more about phishing email), a suspicious attachment, please report the email to security@ubc.ca, and include the email as an attachment. In the case of virus-infected emails, please provide the name of the virus as identified by your anti-virus software.

- Threatening or harassing emails should also be reported to your manager, supervisor or local HR representative.

- Maintain the security of your email account by keeping your password confidential and remaining vigilant against phishing emails. See https://privacymatters.ubc.ca/phishing-emails.

- All written communications and documentation, including emails, may be requested under the *Freedom of Information and Protection of Privacy Act*. Do not put something in writing you would not be comfortable being on the front page of *The Vancouver Sun.*

- Do not forward your UBC email account to your personal email account. All UBC communication must be undertaken with your UBC email.

- See the UBC Fact Sheet on Privacy of Email Systems for more information: https://universitycounsel.ubc.ca/files/2015/05/Fact-Sheet-Privacy-of-Email-Systems.pdf

- UBC is required to ensure that personal information in its custody or under its control is stored and accessed in Canada. You can find more information at https://universitycounsel.ubc.ca/files/2015/05/Fact-Sheet-Privacy-of-Email-Systems.pdf.

Confidential Content Disclaimer:
The following disclaimer should be added to the bottom of any e-mail that is **confidential** in nature:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you are not the intended recipient, any review, use, distribution, copying, retention or disclosure of this message is strictly prohibited. If you have received this message in error, please notify the sender immediately by email and delete this message. Thank you for your cooperation.'

3. Two Way Radios

3.1 Communication via radios is to be brief, clear, precise and kept to work related content only.

3.2 Appropriate and respectful language is to be used throughout all radio communications and free of any libelous, defamatory, offensive, racist or obscene references or remarks.

3.3 While walking throughout hallways, classrooms, offices and shared spaces, turn audible volume to minimum as to not disturb others. Use an ear piece to avoid having staff, faculty and students from hearing broadcast content of radio transmissions, which can disrupt their phone conversations.

4. System Monitoring

If there is evidence that you are not adhering to the guidelines set out within this policy UBC has the right to access the emails on your UBC email account without your consent. For further information on system monitoring, refer to UBC IT Policy http://universitycounsel-2015.sites.olt.ubc.ca/files/2019/08/Information-Systems-Policy_SC14.pdf

5. Questions

Please contact your Manager or Director if you have any questions or concerns regarding the Facilities Communications Policy. If you do not have any questions, Facilities presumes that you understand, agree to, and will abide by the rules and guidelines described throughout this Policy.