Electronic Data Onboarding for Casual Employees.

The following guidelines regarding electronic data are intended to provide further guidance for Human Resources staff, not to replace the *"Acceptable Use of Electronic Information Resources"* policy # IM7200. The guiding principles can also be used to assist Human Resources professionals when providing advice to clients.

When familiarizing yourself with UVic's electronic data use policies one of the most important things = to keep in mind is that all of the data from tools issued by UVic (emails, mobile phones, personal home drives, etc.) is that all of the data from these tools is subject to freedom of information requests, investigations and review when necessary. The Freedom of Information and Protection of Privacy Act (FOIPPA) gives individuals a right to access their personal information held by B.C. Government ministries or their service providers, free of charge. For this reason these tools should not be used for personal use. This includes non role based emails. Furthermore, all records of university business belong to the university and are subject to the university's Records Management policy # IM7700. It is important to be mindful that UVic electronic data is not private and it should not be treated as such. If you would not want the data in your email, on you university issued phone or on your university issued home drive then it should not be there.

UVic data should not be forwarded to external email services like Gmail. UVic issued devices should not be used on public Wi-Fi such as in coffee shops or hotels as these connections should be considered insecure. Review the guidance on the Computer Help Desk site for International Travel and Data Security which provides specific information on what to do if a security officer asks to view your device(s). The basic principle is to minimize the data that is on your device when you cross the border, e.g. disable your email account before you leave.