IT Communications Services Governance Framework

PURPOSE

This document describes the IT communications governance framework for University of Saskatchewan (USask). It identifies designated roles within the university that have specific decision-making accountabilities regarding IT communications services. This framework exists to support the university's IT Communications Services Policy and is meant to be read in conjunction with the university's data governance framework.

This framework establishes a well-aligned governance structure by delineating the business and ICT roles and by facilitating holistic and inclusive IT communications services decision-making.

DATA GOVERNANCE ROLES AND RESPSONSIBILITIES

The Data Management Policy and the university's data classifications need to be considered when determining which IT communications services to use if transmitting university data as there may be privacy and security implications. IT communications services should not be regarded as a secure medium for the communication of confidential or restricted data and should not be depended on to retain university data. Data Handling and Storage Guidelines are available to help members of the university community to identify, understand, manage, and use university data appropriately.

The USask data governance framework establishes a variety roles within the data governance organizational structure. Refer to the data governance framework for a description of the roles and a list of the university's data trustees.

Protecting the university's data is a responsibility shared by all members of the university community.

With respect to IT communications services, the Data Trustees and Data Stewards have the following accountabilities.

Data Trustees

Ultimate authority does not typically reside with a single data trustee. Although each data trustee has areas of responsibility and accountability for which they have expertise, these areas generally overlap with each other requiring collective decision making. This includes prioritizing institutional and audience-centric perspectives across the range of IT communications services.

Data Trustees have IT communications services decision-making accountabilities related to the following activities:

- The Data Trustee determines eligibility for IT communications services for their areas of data responsibility, including decisions regarding aspects such as naming standards and provisioning or de-provisioning of accounts.
- The Data Trustee is involved when there is a need to recover evidence while investigating allegations of misconduct and managing actual or potential criminal or civil litigation in which the university is or may become a party.
- The appropriate Data Trustee or their designate must be consulted on decisions regarding unsolicited communication to large segments of the university community (e.g. all students, all faculty and staff, all employees, all alumni). See Appendix A for more information.
- The Vice-President, Administration and Chief Operating Officer is the designated Head and Data Trustee for Freedom of Information and Protection of Privacy matters. The Head has authority for all decisions made on behalf of the university pursuant to the Freedom of Information and Protection of Privacy Policy and under the Act.
    - The Access and Privacy Officer advises on and coordinates freedom of information and protection of privacy matters. See the Access and Privacy section below for more information.
- The Principal Investigator is accountable for all decisions regarding their research data.

Data Stewards

As with the Data Trustees, Data Stewards decision-making responsibilities related to IT communications services impact many stakeholders and decisions need to prioritize institutional and audience-centric perspectives. Data Stewards have IT communications services decision-making accountabilities related to the following:

- The Data Steward determines the appropriate IT communications services for use as part of their business processes and direct business activity to implement the institutional and customer centric perspective accordingly.

- The Data Steward determines appropriate access to IT communications services records when required for urgent/time-sensitive business continuity reasons due to the absence of a faculty or staff member for reasons such as leaves, terminations, or attrition. This also includes decisions around:
    - Email
    - Messaging and Collaboration Platforms
    - Portals, websites, and web domains

Information and Communications Technology/CIO

The Chief Information Officers (CIO)/AVP Information and Communications Technology ensures the integrity of the university's technology infrastructure. The CIO/AVP partners with the Data Trustees and Data Stewards to support the needs of the administrative and academic units while keeping these critical services stable.

- ICT will provide guidance, procedures, recommendations related to USask's IT communications services as needed to support the priorities of the institution.
- ICT will only access or provide access to IT communications records that have been requested under LAFOIP (through the Access and Privacy Office), under court order, or for exigent business reasons (e.g. absence of a faculty or staff member for reasons such as leaves, terminations, or attrition or fraud investigations) following due process and in consultation with the Data Trustee as appropriate. When possible, account holders will be notified promptly when their IT communications services records have been accessed.

Strategic Communications/CCO

The Chief Communications Officer (CCO)/AVP Strategic Communications ensures the integrity of the university's visual identity, brand, and narrative in all its forms, through all media, with oversight of a wide range of communications, public relations, marketing, and digital outreach activities that promote the university, its programs, and its people. The AVP Strategic Communications and CCO provides campus-wide leadership and vision to support and advance institutional reputation and strategic institutional objectives. For this reason, the CCO offers guidance and advice relating to IT communications services records. As the university's chief communications officer works closely and collaboratively with the senior university administration, academic deans, and other leaders to develop and oversee an integrated, strategic, and institutional communications strategy.

- Strategic Communications oversees (approves) all USask related institutional social media accounts and approves the creation of new USask marketing channels through external services.

General Counsel Legal Office

Access and Privacy

The Access and Privacy Officer advises on and coordinates freedom of information and protection of privacy matters. The Access and Privacy Officer, in consultation with the appropriate colleges, departments, and administrative units, the Head and others as required, is responsible for responding on behalf of the university to all requests for information. The Access and Privacy Officer will also provide advice to colleges, departments, and administrative units relating to freedom of information and protection of privacy issues, including how they pertain to IT communications services records.

- Access to IT communications services records can be requested under the Local Authority Freedom of Information and Protection of Privacy Act, or by court order.
- Access to IT communications services records may be required to recover evidence while investigating matters concerning appropriate use (e.g. harassment, fraud) and managing actual or potential criminal or civil litigation in which the university is or may become a party.
- Access to IT communications services records may also be required for urgent/time-sensitive business continuity reasons due to the absence of a faculty or staff member for reasons such as leaves, terminations, or attrition.

All information about an identifiable individual is personal information and must be dealt with in accordance with the Local Authority Freedom of Information and Protection of Privacy Act. This includes personal information contained within IT communications services records. Personal information does have degrees of sensitivity associated with it. Some personal information, such as phone numbers, has lower sensitivity than other personal information, such as social insurance numbers, which has higher sensitivity.

The Access and Privacy Officer can provide assistance regarding IT communications services records and decisions including:

- Identifying who should have access to a user's account.
- How often the university reviews who has access.
- Identifying who can approve a request for access.
- Developing the process used to approve and provide access.
- Providing guidance on identifying who must be consulted before account access (i.e. content) is granted and determining the appropriate access to service contents (e.g. email messages, chat messages, text messages, etc).

- Providing guidance on identifying who must be consulted before message forwarding and/or message auto-replies can be provided.

Canada's Anti-Spam Legislation (CASL)

Each college, department, and unit at USask is responsible for ensuring that its outgoing electronic messages (including email, text messages, automated telephone messages, or social media messages) comply with CASL. Compliance is overseen by University Communications. It is important to have a proper records management or customer relationship management program in order to record consent; if challenged under CASL, the onus is on the university to establish proof of consent.

Individuals Who Use IT Communications Services

Members of the university community have responsibilities both as individuals and in relation to their affiliation and role with the university. Individuals may have multiple affiliations, but their primary affiliation, combined with their role, will determine their responsibilities. The affiliation hierarchy is outlined in the next section.

- Members of the community will determine how they want to identify, separate, and remove unwanted and unneeded junk mail, non-records, transitory information, and personal mail, chat, or text messages from their IT communication services.
- Members of the community will determine if they want to make personal use of IT communications services given that it is a university service and subject to access requests. Personal use must not compromise the business of the university, must not increase the university's costs, must not expose the university to additional risk, must not damage the university's reputation and must not be part of an activity that the account holder does for personal profit.
- Faculty and staff will, in consultation with their business unit, determine which of their communications records are required for records retention purposes.

Affiliations, Roles, and Accounts

Affiliations are broad categories that define the different types of relationships that an individual may have with the university (e.g. faculty, staff, student, alumni, etc.). An individual may have more than one affiliation. Affiliations are used to group community members who have similar needs at a high level.

Roles are tied to the duties we perform in relation to our affiliation with the university. Roles could include instructor, researcher, analyst, director, etc.

The members' affiliation(s) and role(s) with the university determine the type of IT communications services to which they have access, the duration for which they have access to those services, and their associated responsibilities for use of the services.

The relationship individuals have with the university changes with time. Individuals transition through different affiliations with the university, from student to alumni, employee to retiree, and even through different types of employment relationships, from student marker to intern, staff to sessional lecturer, student marker to faculty member. Members of the university community can (and do) have multiple affiliations with the university. For example, an individual can have both a student and a staff affiliation or a staff and an alumni affiliation. Individuals can also have multiple roles, for example if an individual holds jobs in two different departments simultaneously. However, at any given time, a member can have only one primary affiliation. The Data Trustee for an individual's primary affiliation makes the final decisions related to their IT communication services.

University Accounts

As stated in the university's Information Technology Use Policy "Access to the university's IT services and infrastructure is primarily authorized and provided through an account issued to each individual. Accounts and authorization are not transferable. The person to whom authorization is granted is responsible for all use of that account and is expected to take reasonable steps to ensure the security of the account. Public access to IT services and infrastructure typically does not require an account."

Network Services ID (NSID)

The university provides members of the community with a Network Services ID (NSID) that is used as a username to access university computer and network services such as PAWS, email, collaboration services, computer labs and password-protected webpages. The services you are eligible for depend on your affiliation and role at the university.

The university provides individuals **with a single NSID account**, even when they have multiple affiliations (e.g. faculty, staff, student, alumni). Individuals might also be provided with functional/role-based accounts, depending on their role with the university.

Role-based or Departmental Accounts

Special purpose NSIDs may be created to address the needs for a particular role (e.g. President, Vice-President), function, organization, or IT system to access university computer and network services. These NSIDs may be shared by storing data in a central location that can be accessed by multiple individuals if necessary. They can provide joint access to voicemail and file storage and are an alternative to mailing lists. Role-based accounts can help with records management for senior leadership roles or roles that experience regular turnover. Records management responsibilities may be different for role-based or departmental accounts depending on their purpose.

Appendix A – Approvals for Unsolicited Communications to Large Groups

All official USask communications platforms hosted on university systems are subject to the IT Communications Services Policy.

The university uses many communications platforms that are automatically created and maintained based on individuals' affiliation or role with the University of Saskatchewan. These platforms contain specific identifiable groups, such as all faculty and staff, all students, all faculty, departmental staff, or class lists of students. Individuals may not request removal from the lists within these platforms and for that reason all mass communications sent to through these platforms will be considered unsolicited.

The appropriate Data Trustee or their designate must be consulted on decisions regarding unsolicited communication to large segments of the university community (e.g. all students, all faculty and staff, all employees, all alumni).

Approvals for Unsolicited Mass Communications (Examples)

The following levels are established for the creation and use of involuntary communications platforms. These are very broad categories and are intended as a guideline in making decisions regarding appropriate units and Data Trustees for approving mass communication.

Audience Type	**Approval**	**Usage Examples**
All USask faculty, staff, students, researchers	Vice-President, University Relations	University-wide, general announcements
	Crisis Management Team	Emergency announcements
	Data Trustee for the service impacted	Service outages, service changes
Students	Vice-Provost, Teaching, Learning and Student Experience	Information specific to students.
Alumni	Vice-President, University Relations	Notification of events. Notification of programs and services for alumni.
Faculty and staff	AVP People and Chief Human Resources Officer	Information specific to faculty and staff or retired faculty and staff.

All students within a college	The Dean of the college	Notification of events, programs, or services for students in the college.
All students within a class	The instructor of the class	Class notes. Notifications of class events.
Employees of a college or department	The Dean or Department Head	Notifications of special events.

Operationally, approval within a business unit may be delegated.

Appendix B: Definitions

- **IT Communications Services** – Services that provide the ability to communicate electronically. These include, but are not limited to:
    - Email and calendar services
    - Telephone and voice messaging services
    - Text messaging, instant messaging, and group messaging services (i.e. real-time messages)
- **University-provided IT Communications Services** – IT communications services that the university provides in-house or that the university has arranged from a vendor under a contract. These services may be located on or off premises, but the university is always responsible for the security and privacy of information in its control, regardless of the choice of vendors or location of vendor services.
- **University owned** – Assets purchased by university funds including research grants administered by the university or acquired by the university through some contractual agreement.
- **Record** – Recorded information in any media or format that is created or received and retained in the operations of an organization or person as evidence of functions, policies, decisions and other activities of that organization or person. Records include, but are not limited to, documents (e.g. letters, memoranda, email, contracts, invoices, reports, minutes, publications); images (e.g. photographs, maps, drawings); audio and video recordings; and compiled, recorded or stored data (e.g. audit trails).
- **University record** – A record that is created or received and retained in the operations of a university unit.
- **University data** – Data that is created, collected and stored (either electronically or in hard copy) by units and members of the university community, in support of academic, research, and administrative activities.
- **Account** – An account typically consists of a username—called the Network Services Identifier (NSID)—and a password. This single digital identifier helps to provide a seamless transition between university IT services. The account provides role-based access to university computer and network services. The university sometimes provides access to other types of accounts through a corporate contract or other arrangements.
- **Affiliation** – Broad categories that define the different types of relationships that an individual may have with the university (e.g. faculty, staff, student, alumni, etc.). An individual may have more than one affiliation.
- **University community** – All students, employees, faculty, postdoctoral fellows, alumni, agents, contractors, authorized guests, and persons or organizations acting for or on behalf of the university.