Seat Assignment Agreement

Between

Queen's University – Arthur B. McDonald Canadian Astroparticle Physics Research Institute

And

Grantee: _____

For

Graduate Student and Post Doc Office Stirling Hall Within Rm 412

By signing this Agreement, you (the Grantee), acknowledge that you have reviewed all the information below and agree to the rules and requirements for occupying the assigned seat within the McDonald Institute Offices. The seat assignment provided to you by the McDonald Institute is considered to be a privilege not a right. Your seat assignment is granted for one (1) academic year and must be renewed annually on the date of signature on this agreement. Prior occupancy does not guarantee renewal of the seat assignment. The McDonald Institute Administrative Centre will provide you with information related to the renewal of your seat assignment 60 days prior to the renewal date. For the purposes of this Agreement a "Grantee" means an individual who has been assigned a seat within the McDonald Institute Graduate Student and Post Doc Offices, more specifically described as room 412 Stirling Hall, Queen's University. The seat assignment is Grantee specific, and is more accurately identified as seat number _____ highlighted on attached Schedule A.

To maintain an atmosphere conducive to all individuals sharing the space it is imperative that the guidelines contained within the attached McDonald Institute Graduate and Post Doc Handbook and this Seat Agreement are observed.

Non-Disclosure and Confidentiality Agreement

The Grantee will execute the Non-Disclosure and Confidentiality Agreement affixed hereto as Schedule C. The Grantee acknowledges that they have received and executed a copy of said Agreement.

Acceptable Use of Information Technology Resources Policy

The Grantee will be permitted to use the Queen's University network for computing requirements subject to the following conditions:

1. The Grantee indemnifies and holds harmless Queen's University from any and all claims, demands and costs for damage resulting from a loss of service for any reason
2. Service provision will cease upon the expiration of this seat Agreement
3. Service shall be limited to use of the network only and does not entitle the Grantee to the use of any site licenses or software
4. The Grantee agrees that provision of service is subject to Queen's University Acceptable Use of Information Technology Resources Policy and Queen's University Network and Systems Security Policy attached hereto as Schedule D. Queen's University has the right to terminate this seat Agreement upon any violation of any of these policies. The Grantee also agrees that these policies may change from time to time and that the Grantee will be bound by any and all changes to these policies.

Seat Plan Directory

The McDonald Institute Administrative Centre will develop and maintain a seat assignment directory that will be posted in room 412. As Grantee's acquire/relinquish their seats the directory will be updated.

Seat Assignment

The McDonald Institute Administrative Centre is responsible for assigning Grantee's their seat. Requests for a seat are to be made to the Administrative Centre by email at physparc@queensu.ca. Seats are assigned on a priority basis. It is understood that at times there will be more demand for seats than the McDonald Institute will be able to provide. The McDonald Institute Administrative Centre is responsible for seat assignment prioritization.

If the Grantee is dissatisfied with the seat assignment a request for reassignment can be made to the McDonald Institute Administrative Centre. Whenever possible reassignment will be accommodated.

The seat assignment cannot be used for any other purposes than for which it was intended under the direction of McDonald Institute.

The Grantee may at not time assign/share their seat assignment with any other user (s) without first seeking and securing approval from the McDonald Institute Administrative Centre.

Access

All Grantees will be provided a key to access the space at their discretion. The key will be signed for by the Grantee. If a key is lost a replacement will be made for $10.00.

The Grantee will be permitted 7/24hour access to room 412 and to their seat assignment within 412. Access to the building/Stirling Hall will be Monday to Friday between the hours of 7:00 am and 10:00 pm. There is no sign in/sign out procedure.

Written permission from the McDonald Institute Administration Centre must be obtained prior to use of the seat by non-Grantees. All guests must be accompanied by a Grantee and adherence of guests to the guidelines of

this Agreement while in the McDonald Institute Offices is the responsibility of the Grantee.

Trash/Recycling

Grantees are responsible for the cleanliness of their workspace and for the disposal of trash and recycling in the proper receptacles.

Cubicle and Office Furnishings

The Grantee is responsible for ensuring the furnishings provided are respected and kept in clean working order. All furnishings must be used for their intended use only. The assigned seat is to be maintained as office space, not storage space. The Grantee shall have no right whatsoever to add to or remove fixtures or make improvement to the seat assignment, common or meeting room areas.

Shared Use Meeting Room

The McDonald Institute Administrative Centre provides a communal group meeting space within room 412. The meeting room space must be booked through the McDonald Institute Administrative Office though email at physparc@queensu.ca. The calendar for 412d can be viewed at https://mcdonaldinstitute.ca/412d/. Room booking conflicts will be adjudicated by the McDonald Institute Administrative Office. The meeting room is a shared space and use of the meeting room by Grantees is on a first come, first served basis. No food, drinks, books/documents, or personal items should be left behind in the meeting room. Any belongings left behind may be removed and discarded. Complaints about the use or maintenance of the meeting room must be referred to the McDonald Institute Administrative Centre by email at physparc@queensu.ca.

Repairs/Maintenance

Requests for repairs and/or maintenance to seat assignment or meeting room should be submitted to the McDonald Institute Administrative Centre. Excessive damage to cubicle/office space or furniture by Grantees may be grounds for loss of access to room 412 and cost recovery may be instituted. If a maintenance emergency occurs after core business hours the Grantee will contact Physical Plant Services Fix-It at 613 533-6757 (internal 77301) or fixit@queensu.ca. The Grantee will also contact the McDonald Institute Administrative Centre of any after hours maintenance emergency work requested.

Respect for Others (the Student Handbook, once completed, will be available and affixed hereto as Schedule B):

The space you have been provided is intended as a professional research setting and what follows are guidelines regarding the use of that space.

Respect Another's Need to Work

Just because others are sitting nearby doesn't mean that they are available for conversation at all times. Respect one another's privacy. Act as if there is a door between you and if they appear to be busy, ask if they have a moment to talk.

Be Aware of Smells:
Within open work spaces smells can be magnified. Use consideration when packing your lunch or snacks. Try to eat meals elsewhere rather than at your desk. Many people have allergies to scents, please forgo wearing perfumes, cologne or strong scents in the workspace. Please also pay attention to your personal grooming as well.

Keep Noise and Distractions to a Minimum:
Noisy conversations either between colleagues or on the telephone, or habits such as fidgeting, humming, pencil tapping, pacing, or using a

speaker phone can create a distraction for other users of the space who are trying to concentrate. If you would like to listen to music, podcasts or videos please use headphones or ear buds. When in the unit please turn your personal mobile phone to vibrate or silent. If your chair squeaks ask the Administrative Centre to have it fixed.

Children and Animals in the Workspace:
Please do not bring children or animals to the workspace unless you have explicit permission which can be secured through the McDonald Institute Administrative Centre.

Be Tidy:
A messy desk can be a distraction to others and will detract from the professional image of our organization. Please keep your belongings confined to your own personal space and tidy up your immediate area each day before leaving the unit. Personalization of your space is encouraged but please take into account those working around you and ensure the appearance, effectiveness and safety of the space is not compromised.

Respect Another's Space:
Just because another's workspace is within reach of your desk doesn't make it common domain. Please treat each person's space as if it was a private office. Do not help yourself to anything on other person's desks - ask first if you need a pen or a stapler. Sometimes you are going to hear information not intended for your ears. Act as if you didn't hear it and don't add to the noise level by repeating it.

Don't Come to the Unit if you are Unwell:
When you work in close quarters, it's easy to transfer germs. Stay home if you are sick. Its good hygiene to cover your mouth when you cough, please use the sanitizer provided, and don't leave used tissues around, wipe down your desk, computer keyboard and phone from time to time to help prevent germs from spreading.

Be Considerate:
Respect is key when working in an open common work area. Please act respectful and expect others to act in the same way. Set rules of conduct and reiterate boundaries when they are crossed. It's best to address problems and concerns directly and diplomatically before they escalate. Please remember the McDonald Institute Administrative Centre is always available to assist.

Be Tolerant:
The open work environment brings together disparate personalities. Be tolerant of these differences and find ways to adapt. Everyone is not going to agree with you 100% of the time. Keep an open mind, listen with the intent to learn and focus on the positive aspects of working in a collegial environment. Treat others as you would like to be treated.

Think Like a Team:
In order to maintain a shared open working environment, do not spread gossip, cause another to feel like an outsider or grumble about petty things. You might want to hold regular meetings to share ideas and talk about concerns. Use the suggestion box or engage the McDonald Institute Administrative Centre.

Meeting Rooms:
Use flipcharts and whiteboards provided, leave markers where you find them. Please leave meeting room (s) tidy and ready for use by others.

<u>Notifications</u>

Up-to-date information regarding McDonald Institute seat assignments will be distributed via e-mail.

Grantees are required to provide the McDonald Institute Administrative Centre with accurate contact information, such information will be held in confidence.

Personal Items

Grantees are responsible for any and all items (including, but not limited to personal items) brought into McDonald Institute Office. Personal items should be marked accordingly. McDonald Institute Offices are not immune to theft or vandalism. The McDonald Institute Administrative Centre is not responsible for any items stolen or lost from its Offices. In the event of theft or loss please notify the McDonald Institute Administrative Offices at physparc@queensu.ca and file a report with Campus Security. Campus Security can be reached at 613 533-6111 for emergencies and otherwise at 613 533-6733 or campus.security@queensu.ca.

Smoking and Alcohol/Flammable Materials

Grantees are expected to adhere to all Queen's University policies pertaining to smoking, vaping and alcoholic beverages. Please find links to said policies here: http://irc.queensu.ca/sites/default/files/articles/RE-hamel-smith-smoking-restrictions-in-the-workplace.pdf and http://www.queensu.ca/studentaffairs/sites/webpublish.queensu.ca.vpsaww w/files/files/campusalcoholpolicydec12.pdf. Grantees are not permitted to install small appliances (microwaves, refrigerators, or space heaters) without the written approval of the McDonald Institute Administrative Centre. Flammable liquids, dangerous or controlled materials will not be brought into the McDonald Institute Offices.

Suggestion Box

A suggestion box has been provided in room 412. All suggestions are welcome. The box will be emptied weekly by the McDonald Institute Administrator and responses communicated to the Grantee's via email.

Violations of this Agreement:

All violations of this agreement will be reviewed by the McDonald Institute Administrative Centre and referred to the appropriate University authority.

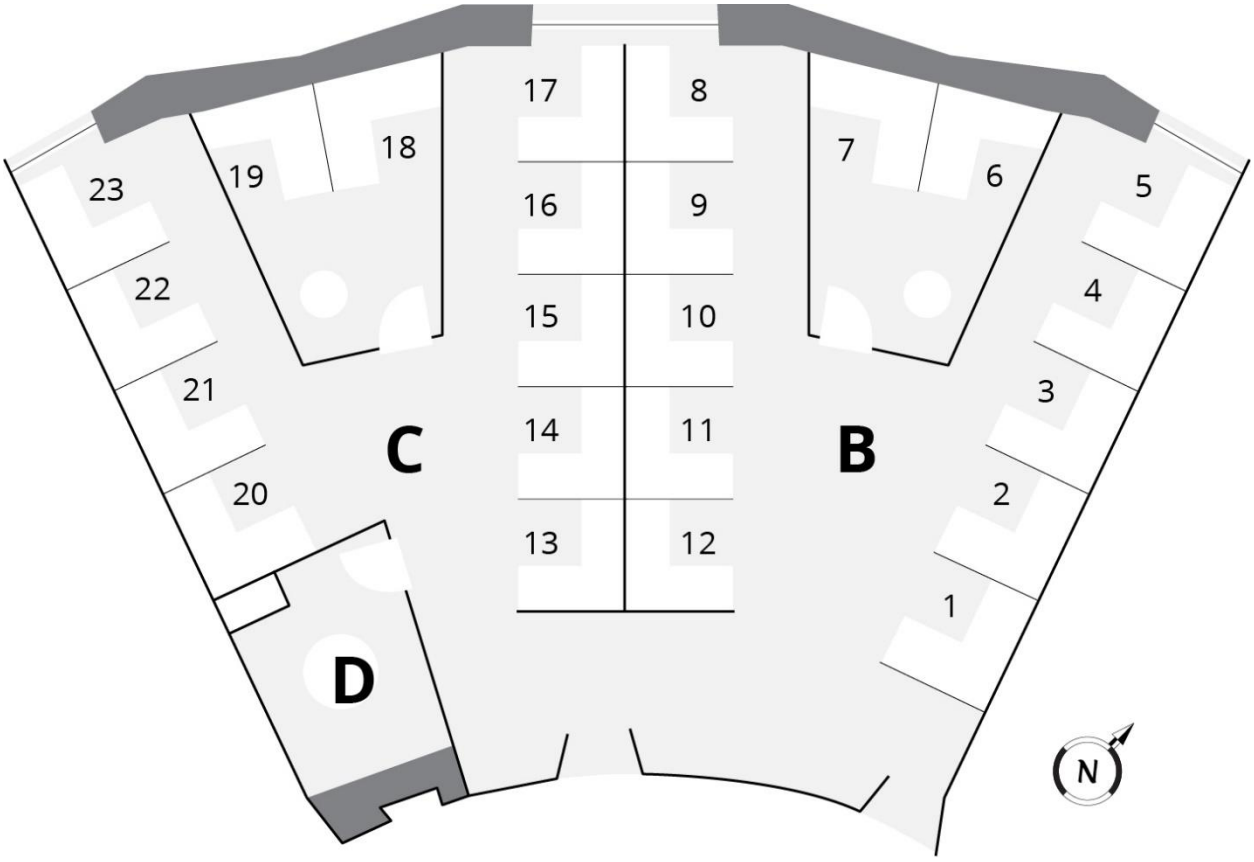
Termination and Re-assignment

It is further understood that the McDonald Institute Administrative Centre may, at any time, and for any reason, terminate and or re-assign this seat Agreement with 30 days written notice to the Grantee.

Arthur B. McDonald
Canadian Astroparticle Physics Research Institute

Queen's University

SCHEDULE A



Arthur B. McDonald
Canadian Astroparticle Physics Research Institute

Stirling Hall 412 B, C, D

Arthur B. McDonald
Canadian Astroparticle Physics Research Institute

SCHEDULE C

CONFIDENTIALITY AND NON-DISCLOSURE UNDERTAKING

This Confidentiality and Non-Disclosure Undertaking is given to Queen's University in consideration of employment provided by Queen's University.

I acknowledge that as part of my employment with Queen's University, I will be given access to information that is of a personal, confidential and/ or proprietary nature, for example: personal information related to staff, faculty and students, such as names, e-mail addresses, salaries, academic and employment information, and/or trade secrets, research data, and credit card or other financial information ("Confidential Information"), for the purpose of fulfilling employment obligations.

I, therefore agree:

- To hold all confidential information in trust and strict confidence and agree that it shall be used only for the purposes required to fulfill employment obligations, and shall not be used for any other purpose, or disclosed to any third party.
- To keep any Confidential Information in my control or possession in a physically secure location to which only I and other persons who have signed a confidentiality agreement with Queen's University have access.
- Not to remove any Confidential Information from Queen's University unless, and to the extent that, I obtain Queen's written pre-authorization. Whenever I am so pre-authorized, I agree to take all necessary steps to keep such Confidential Information secure** and to protect such Confidential Information from unauthorized use, reproduction or disclosure.
- To maintain the absolute confidentiality of personal, confidential and proprietary information in recognition of the privacy and proprietary rights of others at all times, and in both professional and social situations.
- To comply with all privacy laws and regulations, which apply to the collection, use and disclosure of personal information***.
- At the conclusion of any discussions, or upon demand by management, to return all confidential information, including prototypes, code, written notes, photographs, sketches, models, memoranda or notes taken, to Queen's possession and the responsible manager/director.
- Not to disclose confidential, personal and/or proprietary information to any employee, consultant or third party unless they agree to execute and be bound by the terms of this agreement and have been approved by Queen's University in an official, legal capacity.
  I understand that a breach of confidentiality or misuse of information could result in disciplinary action up to and including termination of employment.

I understand that this undertaking survives the termination of my employment relationship with Queen's University.

The laws of Ontario, Canada shall govern this Undertaking and its validity, construction and effect.

I fully understand and accept responsibilities set above relating to personal, confidential and/or proprietary Information.

* Personal Information is any information about an "identifiable individual"

Confidential Information is any information which is designated by the University as confidential.

Proprietary Information is any information which is designated by the University as proprietary like trade secrets, and research data.

Arthur B. McDonald
Canadian Astroparticle Physics Research Institute

SCHEDULE D

Acceptable Use of Information Technology Resources Policy

Category: Administrative

Approval: Senate

Responsibility: Associate Vice-Principal IT / Chief Information Officer

Date: May 27, 2014

Definitions:

The following are definitions for key terms used in this policy:

Term	Definition
Sensitive Information	An electronic set of information or data, such as a database, file or document, that is classified as personal, confidential, or operationally-sensitive, as defined under the Queen's University Data Classification Standard. Whether it is stored on or off campus does not matter.
Unit Head	The Department Head or Director of a Queen's department, or the Principal Investigator or Lead Researcher for a research unit or project.

For other definitions, please see Electronic Information Security Definitions.

Purpose/Reason for This Policy:

The purpose of this Policy is to establish the responsibilities of members of the Queen's community with respect to their use of Information Technology (IT) resources, and those actions necessary or that should be avoided in order to fulfill these responsibilities.

Scope of this Policy:

This Policy applies to all Queen's faculty, staff and students, as well as to contractors or agents engaged by a department or employee, or any individual using Queen's IT Resources, whether on-campus or remotely.

Policy Statement:

The use of Queen's University information technology (IT) resources must be consistent with the academic mission of the University. These IT resources are provided to support the teaching, learning, research and administrative activities of the Queen's community. As a member or guest of the Queen's community, you may have access to valuable internal and external networks and resources, and Sensitive Information, and you are expected to use these resources in a responsible, ethical, and legal manner. Your actions should not adversely affect the ability of others to use these resources, or compromise the security and privacy of sensitive information.

Responsibilities:

You will use Queen's IT resources for the academic and administrative purposes for which they are intended. You will:

a. use only those IT Resources that you have been authorized to use, unless those resources are intended to be generally available to the Queen's community; and
b. not use IT Resources for commercial activities unless such activities have been authorized in writing by the University, and do not adversely impact other users, or introduce risk to the security of personal or confidential information or the Queen's IT infrastructure.

You will not adversely affect the ability of others to use IT resources within or external to Queen's, or compromise the integrity or reliability of those IT resources. You will:

a. ensure that your personal computer or workstation is maintained in accordance with Electronic Information Security Guidelines; and
b. not use Queen's IT resources in a manner that interferes with the normal operation of IT resources within or external to Queen's, or hinders or encroaches on the ability of others to use those resources

You will not compromise the security and privacy of sensitive information. You will:

a. keep your user authentication credentials, such as user accounts and passwords or similar authentication credentials, secure, such that they cannot be used by others;
b. choose secure passwords for your user accounts;
c. preserve the confidentiality of any University information to which you have access in the course of your employment or academic activities at Queen's;
d. preserve the privacy of any personal or confidential information about or belonging to other individuals, to which you have access in the course of your employment or academic activities; and
e. take the necessary precautions to prevent theft or unauthorized use of computers, storage devices, and information.

You will use IT resources in a manner which is consistent with all University policies and does not cause damage to the University. You will:

a. maintain familiarity with Queen's Information Security Policies, Standards and Guidelines, and seek clarification from ITServices about any elements that are unclear; and
b. adhere to the terms of any contractual agreements or arrangements between Queen's University and external service providers or organizations, and use such resources for the intended academic and/or administrative purposes only.

You will not violate the rights of others or contravene the laws of Canada and/or the Province of Ontario in your use of IT resources. You will:

a. respect the copyright and intellectual property rights of others, whether at Queen's or elsewhere;
b. respect the licensing agreements and terms for all software, and only install and use software as permitted in the license agreement for that software;
c. respect the licensing agreements and terms for all electronic resources including databases, journals, books and other print, audio and video content;
d. not use Queen's IT resources for any activities or actions which are illegal or do not comply with Canadian or Ontario legislation; and
e. not use Queen's IT Resources to do anything that is a violation of the rights of others, such as displaying or distributing obscene, harassing, defamatory, or discriminatory material or messages.

You will report suspected, known or observed IT or information security risks or exposures of a serious nature by following the Procedures for Reporting IT or Information Security Incidents or Risks.

Unit Heads are responsible for ensuring that all supervisors, employees, students, guests and contractors are made aware of their responsibilities under the Queen's University Electronic Information Security Policy Framework.

Failure to comply with these responsibilities will be considered a violation of this policy.

Contact Officer: Information Systems Security Manager - ITServices

Related Policies, Procedures and Guidelines: Electronic Information Security Policy, Network and Systems Security Policy, Various related Standards, Procedures and Guidelines

Network and Systems Security Policy

Category: Administrative

Approval: Senate

Responsibility: Associate Vice-Principal IT / Chief Information Officer

Date: May 27, 2014

Definitions:

The following are definitions for key terms used in this policy:

Term	Definition
Sensitive Information	An electronic set of information or data, such as a database, file or document, that is classified as personal, confidential, or operationally-sensitive, as defined under the Queen's University Data Classification Standard. Whether it is stored on or off campus does not matter.
IT Resource	A computer, device, or network on which there is a significant operational dependency for the University, a Department or Research Group, and/or which stores, transmits, or provides access to Sensitive Information. In general this refers to computers functioning as servers, and storage devices such as USB keys and portable hard drives, but also extends to personal computers, printers, facsimile and photocopiers which have internal storage capability that could contain Sensitive Information.
Unit Head	The Department Head or Director of a Queen's department, or the Principal Investigator or Lead Researcher for a research unit or project.
System Administrator	The individual who has primary responsibility for installing, configuring and maintaining an IT Resource. For the purposes of this policy, in the absence of a designated system administrator, the primary owner or user of an IT Resource is regarded as its System Administrator.
Security Controls	Safeguards or measures/countermeasures which prevent, counteract or minimize security risks.

For other terminology, please see Electronic Information Security Definitions and the Queen's University Data Classification Standard.

Purpose/Reason for This Policy:

The purpose of the Network and Systems Security Policy is to ensure the security, integrity and reliability of the University's information technology resources, and the confidentiality of sensitive information, by establishing responsibility for ensuring that IT Resources are installed and maintained in accordance with appropriate security controls, standards and practices.

Scope of this Policy Framework:

This policy applies to all employees of Queen's University who manage IT resources where:

1. There is a significant operational or strategic dependency on an IT resource, at the University, Faculty or Department level; or
2. The IT resource plays a role in storing, accessing or transmitting personal, confidential or operationally-sensitive information.

This policy also applies by extension to external contractors or agents who are involved in deploying and managing IT resources for the University, a department, or a research group.

There is a wide range of IT Resources used across the University. The following policy statement establishes responsibility for ensuring the required security measures are implemented or used for IT Resources:

Policy Statement:

Members of the Queen's Community who are responsible for managing IT Resources on which the University or a Faculty, Department or a research group depend, OR which are used to collect, store or provide access to Sensitive Information, must ensure that those Resources are acquired, installed, configured, maintained and disposed of in a manner that is consistent with Queen's Electronic Information Security Policies, Guidelines and Standards, such that those Resources are not compromised, and sensitive information is appropriately protected. More specifically:

1. ***IT Resources should be installed in locations with physical access controls which limit access to only those individuals who must have it.***
2. ***All servers connected to the Queen's network and providing services should be installed, configured and maintained in accordance with the Server Security Standard and the Electronic Information Security Guidelines.***
3. ***Those individuals involved in configuring and maintaining IT Resources must do so in accordance with the Authentication and Access Control Standard and the Electronic Information Security Guidelines.***
4. ***Those individuals who manage IT Resources which store, access, or transmit Sensitive Information must do so in accordance with the Queen's University Electronic Information Security Policy, the Sensitive Information Protection Standard, and the Electronic Information Security Guidelines.***

5. ***Any new system or software application, whether developed or acquired, that will be used to gather, store, or provide access to sensitive information must undergo a system security assessment prior to being used with real data. This includes both new software applications and when applying major releases/upgrades of those applications.***
6. ***All individuals who manage IT Resources are required to monitor the availability and security of those resources to detect any risks to their regular operation, and to detect any attempts to compromise or access the resource by unknown or unauthorized parties. Logging of access and activity should occur and logs should be reviewed regularly.***
7. ***All software on which there is a significant operational dependency, or which is used to gather, store, process, provide access to, or transmit Sensitive Information, must be acquired or developed in accordance with relevant policies and standards in the Queen's University Information Security Policy Framework.***
8. ***All suspected or confirmed security incidents must be reported in accordance with Procedures for Reporting IT or Information Security Incidents or Risks.***

Contact Officer: Information Systems Security Manager - ITServices

Related Policies, Procedures and Guidelines: Acceptable Use of Information Technology Resources Policy, Electronic Information Security Policy, Various related Standards, Procedures and Guidelines

ORION ACCEPTABLE USE POLICY FOR ORGANIZATIONS

All use of the ORION Network is subject to this AUP. ORANO reserves the right to revise this AUP from time to time, in its sole discretion. When ORANO does so, a revised version will be posted at www.orion.on.ca. The User Organization is responsible for checking that web site from time to time.

1. Purpose of ORION Network

ORION is a Research and Education network that provides an environment in which bandwidth is no longer a major constraint to creativity, innovative research and education projects and/or activities, and new knowledge creation.

ORION provides telecommunications capacity and services to not-for-profit public sector organizations engaged in research and/or education activities ("R&E Organizations") and to other entities that support research and/or education activities of the R&E organizations.

ORION will interconnect with and provide telecommunications capacity and services to other not-for-profit regional, national and/or global entities engaged in research and/or education activities or which support or provide connectivity to R&E organizations.

ORION may provide Internet connectivity and "dim fibre" to the R&E organizations, subject to ORANO approval.

ORION will also serve as a platform for the development and testing of new applications, services and technologies, by the R&E organizations and private sector partners.

ORION is not in the business of providing telecommunications capacity and services to the general public for a financial consideration and will not allow for the resale of its capacity and services by those connected to the network.

2. Eligible Users

Subject to ORANO's discretion on a case-by-case basis, it is ORANO's intent to permit the following types of entities to apply for access to the ORION Network:

- Accredited Ontario universities and community colleges.
- Centres of Excellence, as well as ORANO-approved publicly funded research organizations.
- Government (federal, provincial or local) research institutes or departments, offices of government funded agencies, schools, libraries and hospitals that are connected to an ORION approved PoP or RAN and that are carrying out high bandwidth applications or applications development for research and/or education purposes, shall be eligible to use the ORION Network for these purposes, subject to approval by ORANO.
- Other organizations such as commercial laboratories and businesses, which are carrying out high performance applications or research use, and wish to have access to the ORION Network to connect solely to ORION-eligible research and education users listed above or develop and test new applications and technologies over the network may be eligible, but must have prior approval from ORANO. Such approval may be conditional on the applicant conforming to certain networking requirements and the connection may be of limited duration.

Eligible Entities may be connected directly to the ORION Network through an ORION Network PoP or a third party Regional Advanced Network (RAN) or Community Based Network (CBN). In order to be connected to the ORION Network, RANs and CBNs must provide connectivity to ORION-eligible User Organizations. Only traffic from ORION-eligible User Organization of a RAN/CBN will be accepted by the ORION Network.

3. Limitations on Use

Approval of use of ORION network bandwidth is not guaranteed. ORANO reserves the right to limit inappropriate use of the network. ORANO assumes no liability arising from use of the network or the inability to provide network capacity or services during any outage period.

User Organizations, who, in addition to their usage for research and education purposes, wish to use other applications that may be available on the network, such as the Internet, must apply for and be approved for this use, enter into an agreement with ORANO, and pay an additional fee related specifically to the cost of providing this service. Any such uses may be subject to additional terms and conditions.

The Internet service is primarily an optional service for the university and college participants in the ORION network, and is not intended to be generally available to all ORION network User Organizations.

User Organizations and users of their network capacity and services will not resell ORION network bandwidth or Internet access to the public or any third parties.

User Organizations will not provide network connectivity to third parties except as approved by ORANO.

Use of the ORION Network must be primarily to support research and education activities.

User Organizations must agree that any individuals permitted by such User Organizations to access the ORION Network (i.e., employees, faculty, students, researchers, instructors, etc.) must agree to the restrictions on the use of the ORION Network as contained in this AUP as well as any further restrictions contain in the User Organization's own AUP.

The ORION Network may not be used for any purpose, which is prohibited by or in violation of applicable law.

ORANO reserves the right to (a) block certain IP ports or (b) limit or prohibit certain network applications, particularly as utilization levels increase on the ORION Network.

4. Inappropriate Use

The following guidelines outline certain uses that are not appropriate. The guidelines do not outline all possibilities and therefore are not exhaustive, and ORANO reserves the right to add to the list or make determinations on a case-by-case basis as to whether particular uses are or are not appropriate.

- violates any applicable local, provincial, national or international law or regulation;
- violates any of the accepted norms of the Internet community;
- may damage the reputation and goodwill of ORANO;
- to transmit or store any information, data, text, files, links, software chat, communication or other material that is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, or racially or ethnically hateful including that pertaining to sexual orientation;
- to transmit or store any materials that infringe or can be used to infringe the intellectual property rights of others including but not limited to patents, copyrights, trademarks, service marks or other intellectual property rights;
- use of the ORION network or any attached network in a manner that precludes or significantly hampers its use by others is not allowed;
- connections that create routing patterns that are inconsistent with the effective and shared use of the network shall not be established;
- to harass, threaten, embarrass or cause distress or discomfort upon another user, or other individual or group;
- to circumvent or attempt to circumvent any security measures of the ORION Network;
- post or transmit any unsolicited advertising, promotional materials, or any other forms of direct solicitation; or
- to intercept or access or engage in “sniffing” of packets or in any way interfering with or intercepting the traffic of another User Organization.

ORANO reserves the right to suspend or terminate an individual’s user connection or that of the User Organization should remedial action not be undertaken by the User Organization within a reasonable notice period and dependent upon the critical nature of the inappropriate use. ORANO does not guarantee that it will grant any user or User Organization an opportunity to take remedial action when he, she or it has breached this AUP.

ORANO does not intend to and is not obliged to, but reserves the right to, monitor the content of information transmitted over the ORION Network to protect itself and its User Organizations. If it is necessary to satisfy any law, regulation or lawful request, ORANO may disclose information about any user or any User Organization. Where legally permissible and reasonably practical, ORANO staff will consult with the appropriate User Organization and safeguard the privacy of all those concerned to the extent that it is able.

5. Third Party Definitions and Policies

ORANO is dependent for its ongoing sustainability on User Access Fees and its Membership. It is critical, therefore, that all organizations and institutions using the ORION Network contribute their fair share to ongoing operations of the network. “Third Parties” are normally expected to contribute.

A “third party” is a user entity/organization that obtains its connectivity to ORION through an ORION approved User Organization that has entered into a User Access Agreement with ORANO and has paid its user access fee. Such connections are allowed if there is an explicit written agreement between ORANO and the User Organization providing the connection and also between ORANO and the third party.

Key criteria in determining whether an organization/institution should be considered as a “third party” and pay a separate user access fee include:

- The organization/institution is separately incorporated from the fee paying User Organization through which it is obtaining its connectivity and has its own Board of Directors;
- An organization/institution in which the principal signing/approval authority is different from the fee paying User Organization through which it is obtaining its connectivity; and
- An organization/institution that requires or requests a connection to ORION at the same level as fee paying User Organizations, either separately to the ORION PoP or through a separate connection to a RAN/CBN or fee paying User Organization.

Key criteria in determining whether an organization/institution is not considered to be a "third party" include:

- The connection to ORION is provided by the User Organization in which the organization/institution occupies space in buildings owned by the User Organization and is integrated fully into the IT infrastructure of the User Organization; and
- The organization/institution is a wholly owned operating entity of the User Organization.

Any remedies to which ORANO is entitled that are set out in this AUP are not exclusive. ORANO may take any and all additional actions that it deems appropriate with respect to such activities and reserves at all times all rights and remedies available to it with respect to such activities at law or in equity.

6. Privacy and Security ORANO does not guarantee any user's or User Organization's privacy when it uses the ORION Network. Users and User Organizations should take appropriate safeguards when transmitting confidential information.

November, 2007

Acknowledgement:

I acknowledge and agree to all of the terms and conditions of the Seat Assignment Agreement with the Queen's University- Arthur B. McDonald Canadian Astroparticle Physics Research Institute. A copy of the Seat Assignment Agreement can be found at: https://mcdonaldinstitute.ca/412d/

Dated at Queen's University this _____ day of _____ 2018

_____ _____
Name of Grantee McDonald Institute Witness

_____
Signature

_____
Email Address

_____
Contact phone information

_____
Name of Signing Authority
McDonald Institute Administrative Centre

_____
Signature of Signing Authority
McDonald Institute Administrative Centre