Wellcome Trust Sanger Institute
IT Acceptable Use Policy (AUP) Version 1.9

Introduction

As a user of the WTSI IT Services, IT systems must be used in a reasonable manner and in such a way that does not affect their efficient operation, nor restrict or damage the work of other users.

Users must take all reasonable steps to avoid activities which affect the accessibility, legality, security or viability of the Wellcome Trust Sanger Institute's IT systems. Users are expected to work within the policies and rules defined and approved by the Institute's management and supervisory staff.

The aim of this policy is to help protect the integrity of the IT systems and the Institute's data, from intentional or unintentional damage; to protect the Sanger Institute's reputation and ability to perform its primary functions; and to inform all IT users so that they can meet their responsibilities as outlined below.

Scope

This policy applies to all Wellcome Trust Sanger Institute / Genome Research Ltd (WTSI/GRL) employees, temporary staff, visiting workers, contractors/consultants, third parties, visitors and guests who require the use of WTSI computer facilities.

This policy covers the use of computer networks, computer systems hardware, software, electronic data storage and messaging systems. These computer facilities are collectively known as the IT systems.

Sections of this document may be superseded by the Administrative Rights Acceptable Use Policy, which defines responsibilities and policy for users with administrative access to one or more IT systems.

The Institute reserves the right to investigate and monitor computer use, including internet access, where it believes that (a) there may have been a breach of this or other Institute policies or (b) there is a significant risk of such a breach.

Users of the IT systems who do not comply with the guidelines in this policy and are found to be contravening the AUP will be subject to disciplinary procedures which may result in termination of contract(s) or employment. In minor cases, warnings will be given and access to the IT systems may be restricted. Please see the 'Other Policies' section for information on HR and disciplinary procedures.

Acceptable Use

IT systems at the Institute are provided for scientific research and supporting activities. A user who engages in these activities, and avoids any unacceptable use detailed below, shall be considered to be using the IT systems in an acceptable manner.

Any personal use must not interfere with the primary function of the IT systems, or violate any policy in place at the Institute.

"Acceptable Use" includes the following:

1. The use of IT systems to carry out and support the work of the Wellcome Trust Sanger Institute.

2. Reasonable personal use of IT systems. This should be, modest in amount and must not;
   (a) Interfere with normal operation or the work of other users
   (b) Represent a conflicting interest with the Institute or
   (c) Come under the definition of Unacceptable Use set out in this policy

Internet & Email usage

This policy defines the acceptable use of the Internet/email across the WTSI. The policy applies to accessing the services from the WTSI premises or remotely.

The WTSI internet is connection to the Joint Academic Network (JANET), which is operated by the United Kingdom Education and Research Networking Association (UKERNA) under contract from the Joint Information Systems Committee (JISC). All users of the WTSI wired and wireless networks are therefore subject to the Acceptable Use Policy of JANET (See https://community.jisc.ac.uk/library/acceptable-use-policy for more information).

Internet and Email resources are the property of the WTSI and what we say can be deemed to represent WTSI. Users should not assume that communications are private or secure. Subject to applicable laws regarding employee privacy, WTSI reserves the right to monitor, access, retrieve and review all internet/email activity, and to disclose the nature and content of any such activity to law enforcement officials or other third parties, without any prior notice to employees. WTSI may review internet/email activities for the purpose of:

- Identifying and diagnosing technical problems;
- Preventing system misuse;
- Ensuring 'Reasonable' internet usage, to prevent negative impact on productivity
- Determining whether there have been any breaches of confidentiality or security or violations of the AUP and other WTSI/Janet policies affecting users;
- Investigating misconduct or illegal, unethical or inappropriate activity;
- Assuring compliance with proprietary rights, contractual obligations, licenses;
- Complying with all legal obligations to which the Institute is subject or may become subject;
- Protecting the interests of WTSI

Users must send email through provided WTSI IT systems if sending from an email domain controlled by the Institute, such as sanger.ac.uk.

Under the Companies Act we are legally obliged to display company details on every company electronic communication. The footer is automatically added to outgoing messages. Users must not attempt to circumvent this procedure.

Auto-forwarding of Emails

There may be issues of privacy/security or reliability issues when forwarding emails outside of the Institute; work emails should not be forwarded to personal email accounts unless approved by IT. It is acceptable to forward emails to your home institute address. Please speak to IT for advice prior to auto-forwarding.

Unacceptable Use

"Unacceptable Use" is intended to cover behaviours that may be reasonably regarded as being, or potentially being, unlawful or that will cause undue harm to the Institute, including;

- Deliberate or reckless use of IT systems that may result in the disruption of other users' work, data or privacy
- Offensive behaviour or creation, viewing, downloading or transmission of offensive, obscene or indecent material
- Use, copying, downloading or storage of unlicensed or pirated software
- The use of copyright material without the express permission of the rights holder
- The transmission of confidential or proprietary material from or to parties not entitled to know or possess them
- The unauthorised creation or transmission of unsolicited bulk or marketing material
- Sharing account authentication information, such as passwords, certificates or hardware tokens
- The creation or transmission of material that might bring the Institute into disrepute.

Further information on each point is detailed in the table below.

Unacceptable Use
Deliberate or reckless use of IT systems
• the introduction of malicious software such as viruses , worms, Trojans, adware, spyware etc. • the unauthorised access to facilities or services, or use of WTSI IT systems to facilitate such access ('hacking' and similar offences detailed in the Computer Misuse Act 1990) • the corruption or destruction of other user data, or other disruption of their work • Violating the privacy of other users, accessing their data without permission • Unauthorised modification of WTSI IT Systems, such as modifying the network configuration or cabling of equipment • Accessing confidential data without authorisation • Forging or spoofing emails
Offensive behaviour or creation, viewing, downloading or transmission of offensive, obscene or indecent material
Including, but not limited to; • Pornographic material • Defamatory material • Racist, sexist or other 'hate' material • Material encouraging terrorist activities • Harassment, Stalking, or Bullying activities **Child Pornography** The law on child pornography is very strict: simple possession is a serious crime. **Extreme Adult Pornography** The Criminal Justice and Immigration act 2008 makes it an offense to possess extreme pornography, such as that containing life-threatening violence. Deliberate access of pornographic sites and/or distribution of such material will normally be regarded as gross misconduct under WTSI's disciplinary procedure, and may result in summary dismissal even for a first offence. In some circumstances legal action may ensue.

Use, copying or storage of unlicensed or pirated software

The institute is responsible for ensuring that software in use on WTSI IT equipment is properly licensed. There are legal, financial or reputational consequences for failing a software license audit. Software that requires a purchased license that has not been obtained through WTSI procurement procedures may incur such consequences.

Generally, software must not be installed, used or stored on IT systems unless acquired through the Institute. Software released under free software licenses (such as GPLv2, GPLv3, BSD, etc.) may be used provided the terms of the licence are met and provided its use does not conflict with any other requirement of this policy.

The use of copyright material without the express permission of the rights holder

Including, but not limited to, unlicensed film, TV show and music downloads. The Institute may suffer financial, legal or reputational consequences if found to be storing or transmitting such media. In many cases there is no guaranteed way of determining if media is properly licensed, and so users must not store media where the authenticity may be reasonably doubted.

For this reason Peer to Peer software is prohibited on the network e.g. BitTorrent, uTorrent etc.

The transmission of confidential or proprietary material from or to parties not entitled to know or possess them

Including, but not limited to, the following situations:

- There are groups within the Institute which routinely manage human genetics data. Users who have access to such data must comply with the Human Data Security policy.
- Individuals or groups within the Institute may be subject to a non-disclosure or embargo agreement. The terms of any such agreement must be met.
- Data covered by the Data Protection Act and similar legislation

The unauthorised creation or transmission of unsolicited bulk or marketing material

Transmission of unsolicited bulk communications has repercussions for the Institute as a whole. WTSI has to follow the JANET Acceptable Use Policy, which prohibits unsolicited bulk or marketing material. Violation of the JANET AUP may result in loss of internet connectivity for the Institute and attached groups, which in turn will severely impact the Institute's ability to function.
Sending unsolicited bulk material may also result in the Institute's IT Systems being placed on blacklists, which will prevent further legitimate communication attempts with external people. The Institute will incur financial, time or reputational expenses in these circumstances.

Sharing account authentication information

User accounts with associated passwords are standard practice on all IT systems. Their existence helps the institute to:

1. Protect an individual user's privacy with regard to their stored files and email
2. Protect the work of both individual users and groups against accidental and malicious interference
3. Track software licenses paid for by individual teams
4. Diagnose problems and track activity necessary to diagnose IT problems, or to audit access to controlled data.

A username and password is issued to uniquely identify an authorised person. Access to each individual's account is the responsibility of each user. It is the responsibility of each user to never divulge the password or other private component to an authentication method to anyone or any third party, nor stored it in an insecure manner. This includes passing your credentials to other organisations. Possession of the authentication information does not imply authorisation to use the IT Systems. Unauthorised use may be an offence under the Computer Misuse Act.

Sanctioned shared accounts are subject to additional restrictions outlined in the Shared Accounts Policy. Users must tell the ICT Group if they suspect someone may have acquired their account credentials, such as username and password.

Password guidelines are published on the intranet, visit the Intranet and search for “Passwords & User accounts”

The creation or transmission of material that might bring the Institute into disrepute
The Institute's goals, projects and mission rely on maintaining a high quality reputation within the scientific community. Users must not engage in activities that may jeopardise the Institute's reputation, attract negative public attention or official sanction.

Malicious Software – Viruses, Spyware

Malicious software can destroy or corrupt the Institute's data, preventing proper function of the IT Systems.

Virus checking software is installed by the ICT Group on IT Systems where appropriate. It is there to prevent malicious software when downloading data from the internet, visiting malicious websites, receiving malicious emails or attaching external media to your devices which may contain malware.

Users must ensure that the virus scanner remains enabled at all times, configured as provided, and inform the IT Service Desk if it is disabled. Users should report suspicious emails or software activity to the IT Service Desk.

Computer Misuse

Misuse of computer systems is a criminal offence and can lead to criminal action under the Computer Misuse Act 1990.

Externally visible services

The institute hosts web services that it provides to the general scientific community. Some of these are run by the ICT Group. Other services are run by various groups within the institute. The provision of these services must follow this Acceptable Use Policy, in order to ensure the security and integrity of the institute's reputation and data. Users operating a service for the benefit of others, either internally or externally must ensure that the service is secure, is well maintained, and is not used for any activity listed under 'Unacceptable Use'.

Third-party services arranged by WTSI

This section covers such services as Google Apps for Education. The WTSI Acceptable Use Policy applies to users of these third-party services, when the account is provided by the WTSI, or when the account may be linked to the Wellcome Trust Sanger Institute by branding, email & website addresses, or function. This is to ensure the good reputation of the institute.

Cloud storage, such as the corporate Google Drive should be used for work matters rather than a personal Google Drive. WTSI is not responsible for backing up data stored in the cloud. Users must take responsibility for their own data integrity and security with these services, e.g. storing sensitive and/or confidential data in third-party cloud services (which may cause embarrassment to the institute and/or a breach of the Data Protection Action (DPA) if compromised) should be avoided.

Contracts for IT equipment, software and services

Users must not enter into agreements on behalf of the Institute to buy IT equipment, software or services, except by prior arrangement with the Information & Communication Technology (ICT) team. Such tools and services are evaluated on a case-by-case basis by ICT for potential risks to data and IT system security, impact on the network, and compliance with the AUP and JANET requirements. Due to software licensing requirements and audits, all software must be purchased through the ICT.

Other Policies that also apply

- JANET Acceptable Use Policy: https://community.jisc.ac.uk/library/acceptable-use-policy
- Users of the wireless networks, including visitors to the site, are obliged to accept the Wellcome Trust Genome Campus, Acceptable Use Policy
- Eduroam users will automatically connect to the Eduroam wireless network, and are required to follow the Eduroam Acceptable Use Policy
- Administrative Rights Acceptable Use Policy
- Users working with human genetics data should be familiar with the Human Data Security Policy
- The Institutes Dignity at Work (Bullying and Harassment) policy covers workplace behaviour, including when using the IT systems
- The Institutes Blogging policy covers the WTSI position on staff use of social media:
- The Institutes disciplinary policies and procedures are covered in the Disciplinary and Work Performance Policy

Changes to the AUP

All users should be aware that the most recent version of the AUP, which supersedes all previous versions, is published on the WTSI intranet. Users are responsible for familiarising themselves with the latest version and for complying with AUP requirements at all times.

Key Terminology

ICT – The Information & Communication Technology group is responsible for core IT duties, and runs the IT Service Desk

WTSI / the Institute - The Wellcome Trust Sanger Institute

User / Authorised User - You are considered an 'authorised user' if you have a personal user account allocated to you by one of the Information & Communication Technology (ICT).