Introduction

The 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. In particular users must take all reasonable steps to avoid any activity that affects 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 Board of Management and implemented by the institute’s management and supervisory staff.

The aim of this policy is to help protect the integrity of the IT systems and 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, visitors, guests and contractors who require 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 information technology systems (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Sections of this document may be superseded by the Administrative Rights Acceptable Use Policy, which defines responsibilities and policy for users with administrative access to one or more IT systems.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.

Key Terminology

SSG - The Systems Support Group is responsible for core IT duties, and runs the IT Helpdesk

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 Systems Support Group (SSG).
Account Sponsor - A WTSI employee responsible and accountable for the use of IT systems by visiting workers, external collaborators or contractors.
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 (1) interfere with normal operation or the work of other users. (2) represent a conflicting interest with the Institute or (3) come under the definition of Unacceptable Use set out in this policy.

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.

“Unacceptable Use” is defined as the following:

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

Further information on each point is available later in this document.
Unacceptable Use in detail

1 – Deliberate or reckless use of IT Systems that, with reasonable likelihood, will result in the disruption of other users' work, data or privacy

Such as:
- the introduction of malicious software such as viruses or worms
- 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

2 – 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

The Institute aims to provide a safe and encouraging working environment, and would also suffer reputational consequences if involved in such behaviour listed above. The Institute will act appropriately to any unlawful activity, or any activity that results in a hostile working environment.

Child Pornography
The law on child pornography is very strict: simple possession is a serious crime. The Wellcome Trust Sanger Institute will respect the law in any circumstances where this is found.

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. The Wellcome Trust Sanger Institute will respect the law in any circumstances where this is found.
3 - Use, copying or storage of unlicensed or pirated software

The institute is responsible for ensuring that all 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, and as such 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 license are met and provided its use does not conflict with any other requirement of this policy.

4 - 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.

5 - 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 Genetics 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

6 – 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.
7 - 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 offense under the Computer Misuse Act.

Sanctioned shared accounts are subject to additional restrictions outlined in the Shared Accounts Policy.

Users must tell the Systems Support Group if they suspect someone may have acquired their account credentials, such as username and password.

For advice about choosing a good password, visit the Intranet and search for “Choosing a Password”

8 - 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.
Failure to Comply

Users of the IT systems who do not comply with the guidelines in this policy and are found to be contravening the above definition of acceptable use 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.

In particular, 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.

Computer Misuse

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

Other Responsibilities

Email

Under legislation contained in the Companies Act 2006 we are legally obliged to display company details as footer on every company electronic communication. The Institute regards all email deliberately sent outside the organisation as company email, and the footer is automatically added to such outgoing messages. Users must not attempt to circumvent this procedure.

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

Malicious Software – Viruses, Spyware

Malicious software can destroy or corrupt the Institute’s data, preventing proper function of the IT Systems. It can take weeks or months of effort and a large financial commitment to restore proper service after an infection by malicious software.

Virus checking software is installed by the Systems Support Group on IT Systems where appropriate. It is there to prevent transmission of malicious software, such as when downloading software from the internet or via inadvertent installation during data transfers from external media such as portable disks and USB drives. Some malicious software can also be installed onto machines via email attachments or included in documents.

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

The institute hosts web services that it provides to the general scientific community. Some of these are run by the Systems Support Group. Other services are run by various groups within the institute. The provision of these services must follow the 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 Google Drive, should not be used for storage of personal data unless it is the only feasible option and the data protection issues have been discussed with the Legal Group in advance. The WTSI is not responsible for backing up data stored in the cloud, as administrative access to these third party services is often limited. Users must take responsibility for their own data integrity and security with these services.

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 SSG. Such tools and services are evaluated on a case-by-case basis by the SSG 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 SSG.

Other Policies that also apply

The Institute's internet connection is provided by JANET, and Users must follow the JANET 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

Users working with human genetics data should be familiar with the Human Genetics 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

### Getting Help

If you need advice or help from the Systems Support Group (SSG) you can contact the service desk by the following methods:

**Telephone Extension 7999**  
**Email:** helpdesk@sanger.ac.uk  
**Web:** https://helpdesk.sanger.ac.uk

The Systems Support Group have implemented a wide range of IT solutions for various tasks, and will be able to provide assistance to get the most effective use out of the Institute’s IT systems. You can also log faults and problems into the service desk by these methods.