CYNAPSE: Acceptable Use Policy

Purpose

The following statements are here to explain and clarify authorization to use the CYNAPSE Platform, uses of the CYNAPSE Platform which are acceptable, and those uses which are unacceptable.

It is important to note that the examples are neither exhaustive nor exclusive. The fact that a certain action is not mentioned does not imply that it is permitted, nor, for that matter, prohibited. Before performing such an action, the user needs to check with the CYNAPSE Service Desk and wait for confirmation.

Scope

These statements apply to all end-users of the CYNAPSE Platform, as well as CYNAPSE staff.

Responsibilities

The CYNAPSE Governance Panel is responsible for this document: to maintain, review, authorise and/or communicate.

The CYNAPSE Service Delivery team are responsible for communicating this policy to new users and for obtaining acknowledgement of their receipt, understanding and acceptance of this policy.

Users are required to accept this policy and respond to any request by the CYNAPSE service delivery team in a timely fashion.

The CYNAPSE Head of Service is responsible for communicating this policy to all their staff and for obtaining acknowledgement of their receipt, understanding and acceptance of this policy.

The CYNAPSE Head of Service is responsible for reviewing this policy at least yearly and putting any recommendations for change to the CYNAPSE Governance Panel and through the document change procedure.

Definitions

See common definitions document here.

Policy Statements

Audit

Platform use patterns, access and data held are subject to audit without any prior warning.

Authorisation

Authorisation to access the CYNAPSE Platform is managed via the CYNAPSE User registration and review process via the CYNAPSE Service Delivery team and under the governance of the CYNAPSE Governance Panel. Creation of accounts will be actioned by Lifebit on request of the CYNAPSE service delivery team.

Referencing

You agree to reference the use of the platform in any publications or related works using the following attribution:

This work has utilised the infrastructure provided by the CYNAPSE research platform supported by the NIHR Cambridge Biomedical Research Centre (NIHR203312) Genomic Medicine theme.

Variable compute and storage costs

You accept liability for variable compute and storage costs incurred by your data and analysis. These are billed on a workspace level to the owner. You understand failure to appropriately apply cost controls on your analysis is not a failure of the platform.

Acceptable Use

A. Users are obliged to report any incidents of possible misuse, or violation of this policy, to the CYNAPSE Service Desk as soon as they are able, so that any necessary steps can be taken to contain and rectify the result of the incident or misuse.
B. Users are obliged to report any discovered weaknesses in the platform or workspace to the CYNAPSE Service Desk as soon as possible, so that any necessary steps can be taken to repair the weakness.
C. All users have an obligation to protect data and systems by following up-to-date recommendations to avoid damage from malware and other malicious programs.
D. Users are to treat all data as confidential unless labelled as otherwise.
E. Users to treat all personal data according to the General Data Protection Regulation 2018 and the UK Data Protection Act 2018
F. Clear Desk Policy: When the user is away from the desk, all confidential and/or personal data is to be removed from the desk and/or secured from view.
G. Clear Screen Policy: When working with Confidential and Personal Data, the user is to ensure that the screen is in a position that cannot be overlooked, and the screen is locked when the user is away from the desk.
H. Users to follow both the Clear Desk Policy and the Clear Screen Policy as defined here, above, or to follow overriding local policy appropriate to your institution or employer, whichever is more stringent.
I. The same standards of confidentiality to be observed for electronically held or generated information as for information held on paper.
J. Users are to use the platform workspace(s) to which they have been allocated, only, and for the designated purpose for which that allocation has been made.
K. Users should ensure that any device used to connect to the CYNAPSE Platform remotely is up to date regarding security patches and is running appropriate anti-malware software.

Misuse

A. Users may not attempt to access any data without the authorisation to do so.
B. Users may not share their account(s), password(s), personal identification numbers, security tokens, or similar information or devices used for identification and authorization purposes.
C. Users must not re-identify data within the CYNAPSE platform (e.g. from their knowledge of particular patients) or attempt to do so or assist any third party to do so.
D. Users may not purposely engage in activity that may harass, threaten, abuse or bully others.
E. Users may not engage in activity that may degrade the performance of the CYNAPSE Platform; deprive an authorised user access to CYNAPSE resources; obtain extra resources beyond those allocated; or circumvent CYNAPSE security measures, unless specifically authorized by the CYNAPSE Head of Service.

F. Users may not download, install or run security programs or utilities such as password cracking programs, packet sniffers or port scanners that reveal or exploit weaknesses in the security of CYNAPSE resources.
G. CYNAPSE facilities may not be used for unauthorised personal benefit, unauthorised political activity, unsolicited advertising, unauthorised fund raising, or for the solicitation of performance of any activity that is prohibited by UK or English Law.
H. CYNAPSE facilities may not be used for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities:
    a. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
    b. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
    c. Creation or transmission of material with the intent to defraud.
    d. Creation or transmission of defamatory material.
    e. Creation or transmission of material such that this infringes the copyright of another person.
    f. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services.
    g. Deliberate unauthorised access to networked facilities or services.
    h. Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
        i. wasting resources;
        ii. corrupting or destroying other users' data;
        iii. violating the privacy of other users;
        iv. disrupting the work of other users;
        v. denying service to other users;
        vi. exposing data to 3rd parties outside the airlock process;
        vii. continuing to use an item of software after CYNAPSE Service Delivery has requested that use cease because it is causing disruption to the platform;
        viii. continuing behaviours found to cause disruption to the platform after CYNAPSE Service Delivery request they cease;
        ix. other misuse of CYNAPSE facilities, such as the introduction of "viruses" or other malware
I. CYNAPSE users must not perform activities with Patient Identifiable Data (PID) on the platform without consulting with the Service Delivery team, and potentially the CYNAPSE governance team. The following are specifically prohibited:
    a. Upload of deanonymisation lists
    b. Crosslinking of datasets outside agreed study scope

Additional Policies and Guidance

All users to abide by any other relevant laws, policies and procedures of their host institution.

Sanctions

Breaches of this policy will be reported to:

- The workspace sponsor
- Principal Investigator (if different from sponsor)

- CYNAPSE Governance Panel

This may result in withdrawal of access for the user, other members of a workspace and in extreme circumstances all workspaces under a sponsor (e.g. Principal Investigator).

Exceptions

There are no exceptions to this policy.

Review Plan

This document is expected to be reviewed on a yearly basis or after an event such that it requires change. This could be the change to another related document or a related requirement.

Changes to this document will be communicated to all registered end-users, and CYNAPSE service delivery members, with the expectation users will adhere to the updated policy.

References

Definitions

Document Controls

Version	Author(s)	Date	Changes
0.0	Keiran Raine	12/07/2023	Initial draft