**Acceptable Use Policy for Validated Researchers**

**Introduction**

This Acceptable Use Policy (AUP) outlines the acceptable uses of the East of England (EoE) Secure Data Environment (SDE). All validated researchers are required to follow this policy being granted access to the EoE SDE platform.

**Brief & purpose**

The purpose of this AUP is to ensure the security, reliability, and privacy of EoE SDE users’ data.

**Scope**

This policy applies to all validated researchers (users) accessing the EoE SDE

**Acceptable uses**

Users must restrict their activities in the EoE SDE solely to research analysis for the authorised research purposes as defined by the conditions of the DAC approval.

Personal use is not permissible inside of the SDE environment.

Users must use EoE SDE resources from secure organisational devices.

Users must logout from the SDE or lock their workstation when away.

**Prohibited use**

Users must not engage in illegal activities (e.g., unauthorised access, data theft).

Users must not access, upload, or distribute offensive, threatening, or harmful content. Offensive content includes hate speech, harassment, or violent imagery.

Users must not use SDE resources for unauthorised activities, including commercial activities.

Users must not upload unauthorised tools without specific approval.

Users must not attempt to upload unauthorised personal information to the environment, to include their own.

Users must not in any way attempt to export, transfer or copy patient data.

**System and network activities**

Users must not attempt to access data or accounts for which they do not have authorisation.

Users will not share account details and/or passwords.

Users must have a working individual email address on the Institution’s standard email domain.

Users must not attempt to circumvent any security or authentication measures, including hacking our services.

**Intellectual property**

Users must respect all copyright and licensing agreements.

**Confidentiality**

Users must protect sensitive and confidential information.

Users must not disclose confidential information.

Users must not attempt to identify individuals from the data within the EoE SDE.

**Report**

Users must promptly report any breach of the policy to the SDE team (cuh.eoesde@nhs.net):

**IG Compliance**

Users must be able to demonstrate that they have undertaken IG training prior to gaining access to the EoE SDE and comply with all applicable law and regulatory standards for the acceptable conduct of research.

**Enforcement**

Users must comply and cooperate with all reasonable instructions received from EoE SDE staff in connection with users’ use of the EoE SDE.

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of access to the EoE SDE and legal action.

**Review and revision**

This AUP will be reviewed annually and may be revised as deemed necessary by the EoE SDE team.

**Agreement**

By accessing and using the EoE SDE you confirm that:

You understand and agree for your use of the resources to be monitored.

You will comply with this AUP and all other related policies.