East of England
SECURE DATA ENVIRONMENT

The East of England SDE SATRE Evaluation

The SATRE framework is a self-assessment tool that supports SDE teams to assess themselves against three core areas (or 'pillars') as well as supporting capabilities:

1. **Information Governance**
2. **Computing Technology**
3. **Data Management**

The East of England SDE team took part in the self-assessment exercise as part of VISTA, to demonstrate implementation of SATRE standards.

In August 2025, SATRE published the East of England SDE's self-assessed evaluation on the SATRE website. SATRE is designed as a self-assessment tool to help SDEs and TREs benchmark themselves against best practice, so this process supports transparency and continuous improvement.

Our involvement is also part of the VISTA programme, a national initiative funded by DARE UK to promote consistency and trust in secure data environments. The East of England SDE was awarded funding as an early adopter of VISTA, helping shape standards for the future. A full breakdown of the East of England SDE's score against the SATRE specification is available here, and below you will find a summary of our scores and assessment for each section of the standard.

Information Governance

This part of the SATRE evaluation looks at the policies and procedures of an SDE or TRE that keep data safe, ethical, and legally compliant.

- **Mandatory requirements** include meeting all legal and regulatory standards, strong risk management, regular audits, secure record-keeping, and making

sure only authorised staff can change policies. It also covers safe onboarding, training, and access for everyone who uses the system.
- **Recommended requirements** focus on strengthening governance, such as regular reporting, keeping quality management records, and recognising external training certificates.
- **Optional requirements** add extra value, for example by using automated quality management tools or providing online training platforms.

Together, these measures build trust and make sure data is handled responsibly at every stage.

Score: 37/37 (against applicable standards)

The score here reflects the East of England SDE's robust governance framework and commitment to data protection. Key strengths include:

- Certification to **ISO/IEC 27001**, the international standard for information security management.
- The East of England SDE has completed the **Data Security and Protection Toolkit** (DSPT), demonstrating its commitment to NHS data protection standards.
- Systematic monitoring of **legal, regulatory, and ethical requirements**, including UK General Data Protection Regulations (GDPR) 2021 and the Data Protection Act 2018.
- Structured **implementation of controls** aligned with legal and contractual obligations.
- **Dedicated staff** and proportionate resourcing **to support governance** and compliance.
- **Version-controlled policies and procedures** are managed securely and updated by authorised team members.

Why this score?
Some areas received partial scores due to ongoing development. These include the introduction of regular reporting dashboards, improvements to training needs analysis, and enhanced collection of quality management data. These are part of the SDE's continuous improvement roadmap.

Computing Technology and Information Security

This part of the SATRE evaluation looks at how the technical environment is set up and kept secure.

- **Mandatory requirements** include preventing data from leaving the secure space, providing clear user guidance and the right software, keeping projects separate, monitoring and controlling networks and infrastructure, encrypting

data in storage and transit, and responding quickly to incidents with timely updates.
- **Recommended requirements** focus on usability and resilience, such as making the workspace familiar and easy to use, automating updates and configuration, regularly testing security, and keeping backups with built-in redundancy.
- **Optional requirements** add advanced features like high-performance computing, access to public software repositories, and enhanced physical security measures.

Score: 56/58 (against applicable standards)

Our SDE scored highly in this area due to its secure and well-documented infrastructure. Key features include:

- **Virtual Desktop Infrastructure** (VDI) that prevents data from being copied out of the secure environment.
- **Researchers use familiar analysis tools** (e.g., Jupyter, RStudio) within a secure, isolated environment that meets NHS data security standards, ensuring data never leaves the platform. The Virtual Desktop can be accessed via a browser or an optional client app for improved performance.
- **Clear documentation** is available through the service portal, including guidance on using the platform and managing data transfers via the Airlock system.
- **Software is updated regularly** as part of the Research Engineering Studio (RES) upgrade process.

Why this score?
Some advanced features such as automated configuration validation, high-performance computing, and training simulations for incident response are still in development or not yet implemented. These areas are being reviewed as part of the SDE's ongoing improvement plan.

Data Management

This section focuses on how data is handled, accessed, and protected throughout its lifecycle in the SDE.

- **Mandatory requirements** include documenting all legal and regulatory obligations, recording and controlling data entering and leaving the environment, limiting access to only those who need it, using strong authentication, and having clear rules for data deletion and output checks.
- **Recommended requirements** strengthen good practice with detailed data handling records, metadata catalogues, limiting outputs to what's necessary, and archiving data in accessible standard formats.
- **Optional requirements** cover useful additions such as single sign-on or location-based access controls, automated output checks, and the option to provide summary or synthetic data

Score: 34/34 (against applicable standards)

The SDE scored strongly in this area, reflecting its commitment to secure, transparent, and well-governed data practices. Key strengths include:

- **Robust processes are in place** to assess the legal and regulatory implications of handling data throughout its lifecycle. The East of England SDE complies with UK GDPR and has Section 251 approval from the Confidentiality Advisory Group (CAG). Privacy notices are published on the data controller's website, and privacy-enhancing technologies (PETs) are used to safeguard data.
- **All data handling decisions are documented** through our Data Access Committee (DAC), with version-controlled records maintained in secure document management systems. Internal audits and clear data retention and deletion processes support transparency and compliance.
- **Data is classified by utility, sensitivity, and purpose**. Project-specific data is provisioned for research, and a catalogue of reusable assets is maintained with appropriate access controls.
- **Data ingress is tightly controlled**. Transfers are only enabled when expected and pre-approved, and any data not listed in a manifest is blocked from entering the platform. This prevents researchers from bringing in unauthorised data and ensures that only the requested data from data providers is allowed to enter the East of England SDE.
- **A two-person review process is used for output checking**, supported by SACRO tooling. Outputs must be non-disclosive unless more detailed content is pre-approved by the DAC and information governance leads.

Why this score?
Some areas, such as automation of metadata cataloguing, statistical disclosure control enhancements, and long-term archiving in standard formats, are still being developed. These are part of the East of England SDE's continuous improvement roadmap.

Supporting Capabilities

This section highlights the services and resources needed to keep the environment running smoothly.

- **Mandatory requirements** include documenting all features and operations, making sure projects understand and cover their costs, having a dedicated support team, and involving the public in oversight where personal data is used.
- **Recommended requirements** add resilience and value by testing business continuity plans, assigning project managers, providing training and feedback channels, tracking costs to ensure sustainability, and offering access to legal and data protection expertise.

Score: 17/18 (against applicable standards)

The East of England SDE achieved full marks in the mandatory requirements of this area, reflecting its strong operational foundations and commitment to service quality. Key strengths include:

- **The platform is designed to keep running** even if one part of the system goes offline. This means users experience minimal disruption, even during technical issues.
- **We regularly test and upgrade the system** in different environments to make sure everything works smoothly. A second version of the platform is also being built to add extra reliability.
- **Each project is supported by a service desk team** and a dedicated project manager. Budget alerts are sent to both project leads and the service delivery team to ensure financial oversight.
- **Access to data is tightly controlled**. Only researchers can access the research space once configured, and data managers operate within project-specific boundaries. Admin engineers require elevated privileges to decrypt data, which triggers alerts in the service platform.
- **All features of the platform are clearly documented**, including how it is built, operated, and secured. Researchers can access user guides and support materials through a dedicated online portal, which is regularly updated based on feedback.

Why this score?
The SDE has demonstrated comprehensive coverage of all SATRE requirements in this domain, with mature processes and infrastructure in place to support secure, reliable, and well-managed research environments.