RIVERMEAD INCLUSIVE TRUST

inspiring the journey for independence together

Access Control Policy

Reviewed: Two Yearly

Signed by: _  __ (Chair of the Trust)

Date: March 2025 Due Date: March 2027

Purpose

This policy outlines the Rivermead Inclusive Trust's approach to access control of its computing facilities. It provides the guiding principles and responsibilities to ensure the Trust's access control objectives are met.

Scope

This policy is applicable across all schools and provisions which make up the Rivermead Inclusive Trust and applies to:

- all individuals who have access to Trust information and technologies
- all facilities, technologies and services that are used to process Trust information.
- all information processed, accessed, manipulated, or stored, in any format, by the Trust pursuant to its operational activities.
- internal and external processes used to process Trust information.
- external parties that provide information processing services to the Trust.
- access to 'private' and 'confidential' data/information is governed by this policy.

There are no restrictions on access to 'public' information.

The policy will be communicated to users and relevant external parties.

Objectives

The Rivermead Inclusive Trust's objectives for this policy are to:

- safeguard the Trust's information from security threats that could have an adverse effect on its operations or reputation.
- fulfil the Trust's duty of care toward the information with which it has been entrusted.
- protect the confidentiality, integrity, availability and value of information through the optimal use of controls.

Policy

The Rivermead Inclusive Trust will provide all employees, learners, and contracted third parties with on-site access to the information they need to carry out their responsibilities in an effective and efficient manner.

Access rights and privileges

- Access rights will be accorded following the principles of least privilege and need-to-know.
- Generic or group IDs will not normally be permitted as means of access to Trust data but may be granted under exceptional circumstances if sufficient other controls on access are in place and the control is auditable.
- Under all circumstances, users of accounts must be identifiable.
- Generic identities will never be used to access confidential data or personally identifiable data.
- The allocation of privilege rights (for example, local administrator, domain administrator, super-user, root access) will be restricted, controlled, and not provided by default.
- Authorisation for the use of such accounts will only be provided explicitly, upon written request from the Trust IT Lead and or CEO, Executive Headteacher, Headteacher, Head of School HR, and will be documented by the system owner.
- Staff user accounts can only be requested in writing, and by using the appropriate forms and authorised via the Trust IT team.
- No access to any staff IT resources and services will be provided without prior authentication and authorisation of a user's account.
- Multi-factor authentication (MFA) will be required log on to all Trust machines.
- Access to IT resources and services will be given through the provision of a unique user account and complex password.
- Passwords used to access Trust information systems are a critical part of the Trust's identity management and must not be shared.
- IT Services staff will never ask you to reveal your password by email, in person, or on the phone.
- Do not use your Rivermead Inclusive Trust account password(s) for any other services you use (for example, Facebook, Twitter). This minimises the impact if your passwords to other services are discovered.
- Passwords used to access Trust information systems must comply with the Trust's password standard.
- Usernames and passwords are for individual use only, and must not normally be disclosed to third parties, whether within or outside the Trust

- Any user knowing or believing that they have disclosed their account details, or who knows or suspects that their email account has been compromised, must contact the Rivermead Inclusive Trust IT support team immediately to outline the situation.

Access control

- Access to confidential, restricted and internal information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreement, and applicable Trust policies and regulations. The responsibility to implement access restrictions lies with the data and systems owners.
- Trust log in credentials will be used as the method to secure access to all resources
- Access for remote users will be subject to authorisation and be provided in accordance with the Remote Access Policy. No uncontrolled external access will be permitted to any network device or networked system.
- The use of cloud-based systems must meet the access control provisions laid out in this policy.
- Evaluation of access controls implemented in any cloud system is performed during the vendor assessment.
- Access rights will be reviewed annually.

Third party access

- Third parties are provided with accounts that solely provide access to the systems and/or data they are contracted to handle, in accordance with least privilege and need-to-know principles. The accounts will be removed at the end of the contract or when no longer required.
- Unless operationally necessary (and explicitly recorded in the system documentation as such) third party accounts will be disabled when not in use.
- Third party access must be set with a defined expiry date provided at the time of the original request and any extension of this must be supported by a new request.

Authentication credentials

- Password issuing, strength requirements, and changing and control will be managed through formal processes and standards.

- Password length, complexity, and expiration times will be controlled through Windows Active Directory Group Policy Objects.

Legal and regulatory obligations

The Rivermead Inclusive Trust and its associated academies has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarised below.

Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Rivermead Inclusive Trust IT team** is accountable for the effective implementation of this policy, and supporting information security rules and standards, within The Rivermead Inclusive Trust
- **The Trust DPO** has executive responsibility for information security within The Tryst. They have responsibility for overseeing the management of the information security risks to the Trust staff and students, its infrastructure and its information.
- **The Trust IT Lead** is responsible for establishing and maintaining The Rivermead Inclusive Trust's cyber security management framework to ensure the availability, integrity and confidentiality of The Rivermead Inclusive Trust's information.
- **Users** are responsible for making informed decisions to protect the information that they process. Users will familiarise themselves with the relevant policies governing the information and systems they access.

Compliance and breach of policy

The Rivermead Inclusive Trust will conduct cyber security compliance and assurance activities, facilitated by the Trust's IT support team to ensure cyber security objectives and the requirements of the policy are met. Wilful failure to comply with the policy will be treated extremely seriously by the Trust and may result in enforcement action on a group and/or an individual. If you have any questions or concerns about this policy, please discuss them with your line manager.

Review and development

This policy, and supporting documentation, will be reviewed, and updated every two year and more frequently when best practice or the legislative/regulatory environment changes to ensure that they:

- remain operationally fit for purpose.
- reflect changes in technologies.
- are aligned to industry best practice.
- support continued regulatory, contractual and legal compliance.

Changes to this policy will be presented to the board of Trustees for review prior to publication.

If you have any questions regarding this policy, please contact the Rivermead Inclusive Trust IT team or the Trust DPO.