INFORMATION SECURITY POLICY

The Rodillian Multi Academy Trust

Summary	Information Security Policy	
Responsible Person/Author:	Head of Governance and Compliance	
Applies to: (please check as appropriate)	**Staff ☒** **Student☒** **Community ☐**	
Ratifying Committee(s)	Audit & Risk Committee	
Available On:	**Compliance Library ☒**	**Website ☒**
Date of Approval	21 June 2021	
Effective from:	July 2021	
Date of Next Formal Review:	July 2024	
Review Period	3 Year	
Status:	Non-Statutory	
Owner	The Rodillian Multi Academy Trust	
Version:	1	

Document Control

Date	Version	Action	Amendments
June2021	1.	Policy created	Reviewed and reformatted

Contents

Introduction

1. The Rodillian Multi Academy Trust ("the Trust") is a public body with a fundamental need to process information. It is important therefore that the Trust has a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and to ensure that confidentiality is respected.

Purposes of this Policy

2. To provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Trust to ensure protection of:

    - The IT infrastructure;
    - Key data and information;
    - Those who have access to or who administer IT facilities;
    - Individuals who process or handle key data and information.

3. The policy is designed to provide protection from internal and external security threats, whether deliberate or accidental by:

    - Defining the Trust's policy for the confidentiality, integrity and availability of its key data and information;
    - Establishing responsibilities for information security.

Scope and Applicability of this Policy

4. This Policy applies to the following:

    - Staff employed by, or working for or on behalf of the Trust or Southway;
    - Students studying in a Trust Academy or Southway;
    - Contractors and Consultants working for or on behalf of the Trust; and
    - All other individuals and groups who have been granted access to the Trust's IT systems and/or key data and information.

Roles and Responsibilities under this Policy

The Trust Board

5. The Trust Board will approve this policy for implementation and delegate authority to implement to the Trust Executive and subsequently Academy Principals.

The Chief Executive

6. The Chief Executive will ensure that the IT team have the necessary support to implement a secure IT Network.

The Director of IT and Data

7. The Director of IT and Data will:

    - Ensure the Chief Executive and Data Protection Officer are informed of any security breaches and any subsequent action taken to resolve the issues and prevent further occurrences.

- Review and authorise, where delegated authority has been made, the procurement resources required to maintain IT network security.

- Review and evaluate, with additional technical support if required, the provisions for IT network security.

- Ensure that the relevant IT Network security measures are in place and kept up to date.

8. Inform the Chief Executive and Finance Director of any issues arising that require investment of resources to maintain the IT network security beyond that agreed within the terms of engagement.

9. Ensure the system is reviewed on a regular basis to ensure that the system is up to date and secure and that no malicious codes, software or viruses are deployed.

The Head of Governance and Compliance

10. The Head of Governance and Compliance will ensure that this Policy is available to Staff and members of Trust Governance and that they are made aware of any revised editions.

All staff and members of Trust Governance

11. It is the responsibility of each member of staff to: -

- Ensure that they have read this policy and the associated documents;
- Attend any associated training as required;
- Act in accordance of this policy and the ICT Acceptable usage policy with respect to IT network security;
- Report any potential IT network security breaches or non-compliance to their Line Manager and the local IT team immediately;
- Speak with their Line Manager if they are uncertain regarding sections of this policy.

12. Non-compliance with this policy may lead to internal disciplinary matters, or could lead to referrals to external agencies as appropriate.

Organisational Security

Third Party Access

13. Access to the Trust's information processing facilities by third parties will only be permitted by the Trust's Director of IT and Data or their nominee.

Assets

14. Inventories of information assets, including both hardware and software will be maintained by the local IT Team and overseen by the Trust Director of IT and Data.

Personnel Security

15. Job descriptions will include specific responsibilities for the protection of particular assets or the execution of particular processes or activities such as data protection.

16. Steps will be taken to minimise the likelihood of personnel, who pose a security risk, being employed in posts involving key data and information, such as those concerned with financial or personnel related data. This will usually be determined through the appointment process, including references and through an enhanced Criminal Records Bureau Check.

17. All members of staff are reminded of their obligation to protect confidential information.

18. The allocation and management of passwords shall be controlled by the Trust. Users are required to follow good security practices in the selection, use and management of their passwords and to keep them confidential

Security Incident Management

19. Users that are implicated in security incidents on the Trust network will have access removed. Subsequent reinstatement of access will only be permitted when remedial action has been taken that ensures the security of the IT network and agreed by the Director of IT and Data.

20. Any computer that is perceived to be placing the integrity of the Trust network or the network of an Academy at risk will be disconnected from the network. Subsequent reinstatement will only be permitted once the security of the computer has been established and agreed by the Director of IT and Data.

21. Events that are regarded as being 'security incidents' will be defined, and processes implemented to investigate, control, manage and review such events. The aim of this process will be to determine the cause of the incident and to prevent further occurrences. If it is deemed that there is fault, then additional consequences may be pursued either through internal policies or through referral to relevant external agencies.

Physical and Environmental Security

22. Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, information assets.

23. Computer systems and networks will be protected by suitable physical and technical security controls including hardware-based firewalls and antivirus software.

24. File servers and machines that hold or process high criticality, high sensitivity or high availability data will be located in physically secured areas.

25. Access to facilities that hold, or process high criticality, high sensitivity or high availability data will be controlled.

Back-up and Data Storage

26. Data on critical systems will be backed up on a daily basis. Backups will be replicated to an offsite location.

27. Key data should be held on a network resource or the Trust's Microsoft365 cloud provision so that it is backed up through a routine managed process. Where this is not possible, provision must be made for regular and frequent backups to be taken.

28. Backup checks and restoration tests will be implemented by the IT team and overseen by the Director of IT and Data.

Disposal of Equipment

29. Removable magnetic and optical media containing key data will be reused or disposed of through controlled and secure means when no longer required.

30. Procedures will be made to ensure the secure disposal of disk drives and disk packs containing key data when these become defunct or unserviceable.

31. Redundant computer equipment will be disposed of in accordance with the **Waste Electrical and Electronic 2013 Regulations** and through secure and auditable means.

Access controls

Permission levels

32. Permission to access the following system and information categories will only be granted to those staff members whose duties expressly require it: -

- Any sensitive documentation;
- Critical system access;
- Key data and information; or
- Live operating systems.

33. The allocation and use of system privileges on each computer platform shall be restricted and controlled by the Director of IT and Data or those to whom delegated authority has been provided.

External access

34. Controls will be implemented to manage and control remote access to key data. Remote access will be monitored by the IT teams and overseen by the Director of IT and Data.

35. Controls will be implemented to check for malicious or fraudulent code being introduced to critical systems and appropriate software will be installed and managed to prevent the introduction and transmission of computer viruses both within and from outside the Academy.

36. Controls will be implemented to achieve, maintain and control access to computer networks, including wireless Local Area Networks. Access may be granted to other parties by the Director of IT and Data, or those with delegated authority, providing that written confirmation of the in-house security protocols to prevent unlawful access are provided and meet requirements.

Unattended User Equipment

37. Users of IT facilities are responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

38. Where available, password protected screen-savers and automatic log-out mechanisms are to be used on office based systems to prevent individual accounts being used by persons other than the account holders, but not on cluster computers that are shared by multiple users.

Monitoring System Access and Use

39. Access to and use of systems will be monitored for both staff and students.

Other Policies

40. This policy should be considered in conjunction with the following Trust policies:

- Data Protection and Information Governance Policy
- ICT & E-Safety Policy
- ICT Acceptable Usage Policy
- Privacy Notices

Monitoring

41. The Head of Governance and Compliance and Director of IT and Data will monitor the implementation and effectiveness of the policy by monitoring reports made under the policy.

Diversity

42. The Trust is committed to a policy of celebrating diversity, promoting equality of opportunity, providing an inclusive workplace, and eliminating any unfair treatment or unlawful discrimination. This overriding objective applies to all policies and procedures relating to staff and students. The Trust will always comply with the requirements of the **Equality Act 2010** and associated guidance produced by the Department for Education.

Appendix 1: Equality Impact Assessment

Equality, Diversity, Cohesion, and Integration Screening.

As a public authority, the Rodillian Multi Academy Trust needs to ensure that all our strategies, policies, service, and functions, both current and proposed have had proper consideration of equality, diversity, cohesion, and integration.

A **screening** process can help judge relevance and provides a record of both the **process** and **decision.** Screening should be a short, sharp exercise that determines relevance for all new and revised strategies, policies, services, and functions. Completed at the earliest opportunity it will help to determine:

- the relevance of proposals and decisions to equality, diversity, cohesion, and integration.
- whether or not equality, diversity, cohesion, and integration is being/has already been considered, and
- whether or not it is necessary to carry out an impact assessment.

Organisation: The Rodillian Multi- Academy Trust	**Department responsible for the Policy:** Head of Governance and Compliance
Lead Person: Head of Governance and Compliance	**Contact Number:**

1. Title: Information Security Policy

2. Please provide a brief description of what you are screening
The Policy

3. Relevance to equality, diversity, cohesion, and integration		
Questions	**Yes**	**No**
Is there an existing or likely differential impact for the different equality characteristics?		x
Have there been or likely to be any public concerns about the Policy or proposal?		x
Could the proposal affect how services are organised, provided, located and by whom?		x
Could the proposal affect our workforce or employment practices?	x	
Does the proposal involve or will it have an impact on: -? • Eliminating unlawful discrimination, victimisation, and harassment • Advancing equality of opportunity • Fostering good relations	 x	 X X

4. Considering the impact on equality, diversity, cohesion, and integration

- **Scope of the proposal:** Students and staff.
- **Who is likely to be affected?** Students and staff.
- **Consultation and engagement activities with those likely to be affected?** The Policy is available through the Trust and Academies websites and a written copy can be provided on request.

- **Key findings**

We have considered the potential positive and negative impact on different equality characteristics in relation to the Policy and do not believe that any groups will be adversely affected. The Trust is vigilant in adhering to the appropriate legislation in relation to protected characteristics and to preventing discrimination. Managers are supported and trained in relation to these areas. The Policy has considered religious, racial and gender-specific clothing requirements and those of staff with disabilities in line with the Equality Act.

We have considered the perception that the proposal could benefit one group at the expense of another and we do not believe that the Policy could be perceived to be discriminatory with regards to its wording or format.

- **Actions**

The Trust will continue to promote positive impact and remove/reduce negative impact through the application of this Policy within the organisation.

5. Governance, ownership, and approval

Please state here who has approved the actions and outcomes of the screening

Name	**Job title**	**Date**
Adam Marham	Head of Governance and Compliance	10.06.21

6. Publishing

This screening document will act as evidence that due regard to equality and diversity has been given.

Date screening completed	10.06.21
Date agreed at Trust Board	21.06.21