drb Ignite Multi Academy Trust

Cyber Security Policy

Contents

Trust Vision

'All pupils achieve the highest standard of educational outcomes regardless of circumstances or background'.

The drb Ignite Trust has been established through a shared belief that lives can be transformed by what goes on in schools. We believe that the process of teaching and learning shapes futures. To this end, our vision is to give every pupil learning experiences that excite and give them the power to begin to shape their own lives.

1. Purpose

The purpose of this policy is to establish a comprehensive framework for managing cybersecurity risks, protecting information assets, and ensuring the safety and security of IT resources across all schools within the drb Ignite Multi Academy Trust (hereafter referred to as 'the Trust'). This policy ensures compliance with the Data Protection Act 2018, the General Data Protection Regulation (GDPR), and the Department for Education's (DfE) statutory guidance.

2. Scope

This policy applies to all employees, pupils, contractors, volunteers, and any other personnel with access to the Trust's information systems and data.

3. Information Security Objectives

- Protect the confidentiality, integrity, and availability (known as the CIA Triad) of information.
- Ensure compliance with legal, regulatory, and educational standards.
- Provide a safe and secure digital environment for learning and administrative activities.

4. Roles and Responsibilities

- **Trust Board**: Approve the cybersecurity policy and ensure adequate resources are allocated for its implementation.
- **Chief Information Security Officer (CISO)/Director of IT and Compliance**: Oversee the implementation and maintenance of the cybersecurity policy across the Trust.
- **IT Services Team**: Implement and manage technical controls at individual schools.
- **All Staff and pupils**: Adhere to the cybersecurity policy and report any security incidents.

5. Risk Management

- Conduct regular risk assessments to identify and evaluate cybersecurity risks specific to the educational environment.
- Implement appropriate controls to mitigate identified risks, including safeguarding measures for student data.
- Review and update risk assessments periodically or when significant changes occur.

6. Access Control

- Implement role-based access controls to ensure users have the minimum access necessary to perform their duties, with particular attention to safeguarding student information.
- Implement local access controls to restrict access to information systems based on geographical locations, ensuring that only authorised personnel can access the systems from approved locations outside of the UK.
- Conduct regular reviews of user access rights, especially when roles change, or staff leave.
- Use strong authentication methods, such as multi-factor authentication, for access to sensitive systems and data.

7. Asset Management

- Maintain an inventory of all information assets, including hardware, software, and data.
- Classify information assets based on their sensitivity and criticality to educational activities.
- Implement appropriate controls to protect information assets throughout their lifecycle, including disposal.

8. Cryptography

- Use encryption to protect sensitive information in transit and at rest, with a focus on pupil records and personal data.
- Manage cryptographic keys securely, ensuring proper generation, storage, and disposal.

9. Physical and Environmental Security

- Implement physical security controls to protect information systems and facilities within schools, such as secure access controls and CCTV.
- Ensure environmental controls, such as fire suppression and climate control, are in place to protect hardware.

10. Operations Security

- Establish and maintain secure baseline configurations for all systems and educational devices.
- Implement procedures for managing changes to information systems, ensuring minimal disruption to educational activities.
- Monitor and review system activities for signs of security breaches, particularly in systems handling student data.
- Conduct regular threat intelligence reviews to stay informed about current and emerging cybersecurity threats.

11. Communications Security

- Protect information transferred within and outside the Trust using secure communication channels, such as encrypted email.
- Ensure third-party service providers adhere to the Trust's cybersecurity standards and sign data processing agreements where necessary.

12. Incident Management

- Establish an incident response plan to handle cybersecurity incidents, including data breaches involving pupil information.
- Train staff and pupils on incident reporting and response procedures.
- Conduct regular drills and reviews of the incident response plan, particularly focusing on potential data breaches and cyber-attacks.

13. Business Continuity and Disaster Recovery

- Develop and maintain a business continuity plan to ensure the Trust can continue operations during a cybersecurity incident.
- Implement a disaster recovery plan to restore critical systems and data after a breach, including prioritization of educational systems.
- Test and update these plans regularly.

14. Training and Awareness

- Provide regular cybersecurity training to all staff and pupils, tailored to the educational environment.
- Raise awareness about current cybersecurity threats and best practices, with an emphasis on online safety and data protection.
- Ensure all personnel understand their role in protecting the Trust's information assets and the specific risks associated with pupil data.

15. Policy Review and Maintenance

- Review and update the cybersecurity policy annually or when significant changes occur, ensuring it remains aligned with current laws and regulations.
- Document and communicate any changes to the policy to all schools within the Trust.

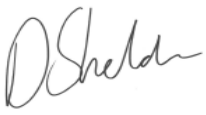
16. Compliance

- Ensure compliance with relevant legal, regulatory, and educational requirements, including GDPR and the Data Protection Act 2018.
- Conduct regular audits to verify adherence to the cybersecurity policy and address any non-compliance issues promptly.

17. Policy Monitoring and Review

The Director of IT and Compliance has overall responsibility for the maintenance and operation of this Policy. The Policy is reviewed annually by the Audit and Risk Committee.

Should there be any changes/further national guidance issued relevant to this Policy, it will be updated accordingly prior to the review date shown above and referred to the next Trust Board meeting.

Monitoring and review:	Board of Trustees Director of IT and Compliance
Staff responsible:	Director of IT and Compliance
Committee responsible:	Audit & Risk Committee
Date approved:	July 2024
Reviewed:	July 2024
Next review:	July 2025
Sign off by Chair of Trust:	 Date: July 2024

18. Change Management

Issue No:	Change date:	Change description:
1.0	July 2024	Initial release