Information Security Policy

Board Approved Date	May 2026
Version	1.8
Author Initials	SW/DP
Review Date	May 2027

Amendments

Policy Date	New Version Number	Summary of change	Comments
March 2021	1.3	13 Remote Learning	
February 2022	1.4	6.4 and 8.1 updated	
March 2023	1.5	Sections 6 and 17 updated	
March 2024	1.6	No changes	
March 2025	1.7	No changes	
May 2026	1.8	Rewrite and restructure of policy	

Contents

1. Introduction

Education South West (ESW) is committed to protecting the confidentiality, integrity, and availability of the information it creates, processes, stores, and shares. Information is a critical asset of the Trust, and appropriate safeguards must be applied to protect it from unauthorised access, loss, misuse, damage, or disruption.

2. Statement of Policy

This policy sets out ESW's commitment to maintaining effective information security controls across all Trust schools and operations. It applies to all information systems, whether managed internally or by third parties, and to all forms of information, including digital, paper, verbal, and visual.

ESW will implement proportionate and risk-based security measures that:

- Protect the Trust, its staff, students, and stakeholders from harm
- Support secure and appropriate information sharing
- Ensure compliance with legal, regulatory, and contractual obligations
- Enable the effective delivery of education and Trust business without unnecessary restriction

3. Scope

This policy applies to:

- All employees, governors, directors, contractors, volunteers, student teachers, and third parties authorised to access ESW information or systems
- All ESW information assets and information systems, including cloud services, networks, devices, applications, and data

4. Legal and Regulatory Compliance

ESW will handle information in accordance with applicable legislation and recognised standards, including data protection, freedom of information, computer misuse, safeguarding, and human rights legislation. Compliance with legal requirements is mandatory for all users of Trust information.

5. Principles of Information Security

ESW adopts the internationally recognised information security principles of:

- **Confidentiality** – information is accessible only to those with legitimate authorisation
- **Integrity** – information is accurate, complete, and protected from unauthorised modification
- **Availability** – information and systems are available to authorised users when required

6. Risk Management

Information security risks will be identified, assessed, and managed in line with the Trust's risk management framework. Appropriate controls will be implemented to reduce risk to an acceptable level, and risks will be reviewed regularly to ensure continued effectiveness.

7. Security of Systems and Networks

ESW will ensure that information systems and networks are protected against unauthorised access, cyber threats, and service disruption. Security controls will be applied throughout the lifecycle of systems, including procurement, implementation, operation, and decommissioning.

8. Protection from Malware and Cyber Threats

The Trust will take reasonable and proportionate steps to protect systems from malware, intrusion, and other cyber security threats, including the application of preventative and detective controls aligned with current best practice.

9. User Access and Authentication

Access to information and systems will be restricted to authorised users with a legitimate business need. Authentication and access controls will reflect the sensitivity of the information and the role of the user. Users are responsible for safeguarding their credentials and complying with acceptable use requirements.

10. Physical Security

Appropriate physical security measures will be in place to protect premises, equipment, and information from unauthorised access, loss, or damage. All users are responsible for maintaining the security of Trust property in their care.

11. Information Asset Management

All information assets are owned by the Trust and must be classified, managed, retained, and disposed of in accordance with Trust policies and legal requirements. Accountability for information assets will be clearly defined.

12. Acceptable Use and Monitoring

Use of ESW information systems must be lawful, ethical, and consistent with Trust policies. The Trust reserves the right to monitor system use to protect users, systems, and information, and to ensure compliance.

13. Home, Remote Working, and Remote Learning

Information security requirements apply equally to home working, remote working, and remote learning arrangements. ESW will ensure that appropriate safeguards are in place to protect information accessed or processed outside Trust premises.

14. Personal Data

All personal data will be processed fairly, lawfully, securely, and transparently, in line with data protection legislation and Trust privacy notices.

15. Third Parties

Where third parties process information on behalf of ESW, the Trust will ensure that appropriate information security and data protection assurances are in place before access is granted.

16. Information Security Breaches

Failure to comply with this policy may result in disciplinary action, contractual remedies, or legal consequences. All actual or suspected information security incidents must be reported promptly and will be managed in accordance with Trust requirements.

17. Incident Management and Business Continuity

The Trust will maintain arrangements for responding to information security incidents and for maintaining critical services in the event of significant disruption.

18. System Change and Development

Information security requirements will be considered throughout the development, acquisition, and change of systems and services to ensure risks are appropriately managed.

19. Review and Governance

This policy will be reviewed at least annually, or sooner if required by changes in legislation, technology, or risk. Compliance with this policy is mandatory and subject to oversight by the Trust.

20. Information Security Standards

Supporting the Information Security Policy

1. Purpose

These standards define the minimum mandatory controls required to support the ESW Information Security Policy. All users and systems must comply with these standards.

2. Identity and Access Control

All users must have a unique account.
MFA must be used where supported.
Access must follow least privilege principles.
Access must be reviewed annually.
Accounts must be disabled when no longer required.

3. Device Security

All devices must be centrally managed.
Devices must use encryption.
Security patches must be applied promptly.
Anti-malware must be active.

4. Network Security

Networks must be protected from unauthorised access.
Firewalls must be in place.
Systems must be patched regularly.
Vulnerabilities must be remediated.

5. Data Protection

Data must be classified and handled appropriately.
Personal data must be protected.
Access must be based on legitimate need.

6. Backup and Recovery

Critical data must be backed up.
Backups must be secure.
Restores must be tested.

7. Monitoring

Systems must be monitored.
Logs must be retained.
Suspicious activity must be investigated.

8. Incident Management

Incidents must be reported immediately.
Incidents must be recorded and resolved.

9. Third Parties
Third parties must be assessed.
Contracts must include security controls.

10. Remote Working
Remote devices must be secure.
Users must prevent unauthorised access.

11. Training
Staff must complete annual training.

12. Compliance
Compliance is mandatory.
Audits will be conducted.
Non-compliance may result in disciplinary action.

Appendix A: Control Mapping

Identity & Access → IASME Level 2 Theme 9 / Cyber Essentials Access Control

Device Security → IASME Level 2 Theme 3 and Theme 10 / Cyber Essentials Devices

Network Security → IASME Level 2 Theme 10 and Theme 12 / Cyber Essentials Firewalls

Data Protection → IASME Level 2 Theme 4 / UK GDPR

Backup → IASME Level 2 Theme 13 / Cyber Essentials

Monitoring → IASME Level 2 Theme 12

Incident Management → IASME Level 2 Theme 14

Third Parties → IASME Level 2 Theme 2 and Theme 5

Training → IASME Level 2 Theme 7