Wylye Valley
Primary School

Love Care Respect

To aspire to being outstanding in everything we do, by always aiming higher.

"Let your light shine in all you say and do."

Matthew 5:16

IT Security, Cyber Protection, and Data Use & Access (DUAA) Policy

1 Introduction

1.1 This policy sets out the framework for managing IT security, cyber protection, and data use at the school in line with UK GDPR, the Data Protection Act 2018, DUAA, DfE Cyber Security Standards, and NCSC guidance.

1.2 It ensures the school protects personal data, maintains system integrity, and manages risks to individuals' rights and freedoms.

2 Scope

2.1 This policy applies to all staff, contractors, governors, and third parties who access or process school systems or data.

2.2 It covers all devices, networks, systems, processes, and third-party services used for school business, including **data shared under DUAA**.

3 Roles and Responsibilities

3.1 **Data Protection Officer (DPO):** Advises on compliance, oversees DUAA data sharing, and ensures risk mitigation measures are applied.

3.2 **Headteacher / SLT:** Accountable for IT security governance, resource allocation, and risk oversight.

3.3 **IT Lead / Provider:** Implements technical controls, monitors security, and responds to incidents.

3.4 **All Staff:** Comply with policies, report incidents promptly, and protect data on all devices and platforms.

4 Access Control

4.1 Systems must use **role-based access**, **least privilege**, and **multi-factor authentication** for sensitive or administrative access.

4.2 Accounts must be regularly reviewed and disabled when no longer required.

4.3 DUAA-shared data must be accessed only by authorised staff in accordance with access agreements.

5 Network and Endpoint Security

5.1 Network devices, firewalls, and endpoints must be configured securely and regularly monitored.

5.2 Anti-virus/anti-malware software must be maintained and updated.

5.3 Remote access must be secure, encrypted, and logged.

6 Information Security

6.1 Personal data must be processed in line with **UK GDPR principles**: lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, storage limitation, integrity, and confidentiality.

6.2 Data shared under **DUAA** must be documented, risk-assessed, and have appropriate contractual safeguards in place.

7 Software and Patch Management

7.1 All software and operating systems must be kept up to date with security patches.

7.2 Unsupported software must not be used for school business.

8 Mobile and Remote Device Security

8.1 All mobile devices must be encrypted, password-protected, and configured to allow remote wipe if lost or stolen.

8.2 Personal devices may only be used in line with the school's **Bring Your Own Device (BYOD) procedures**.

9 Third-Party and Cloud Services

9.1 All third-party services must be assessed for security and **DUAA compliance** before use.

9.2 Contracts must define data protection responsibilities, access controls, and breach notification obligations.

10 Security Awareness and Training

10.1 Staff must receive annual cybersecurity and data protection training.

10.2 Training must include phishing awareness, secure password practices, and DUAA obligations.

11 Incident Reporting and Management

11.1 All suspected cyber incidents, breaches, or unauthorised access must be reported to the **DPO immediately**.

11.2 The **Incident Response Plan** will guide containment, investigation, mitigation, and ICO notification where required.

12 Business Continuity and Disaster Recovery

12.1 Critical systems and data must be backed up regularly and stored securely off-site or in an immutable form.

12.2 Recovery procedures must be tested periodically to ensure operational resilience.

13 Monitoring and Audit

13.1 Systems and networks will be monitored for unauthorised access or anomalies.

13.2 Regular audits and vulnerability assessments must be conducted.

13.3 DUAA data sharing activities must be reviewed periodically to ensure compliance.

14 Policy Review and Updates

14.1 This policy will be reviewed at least annually, or after significant changes in legislation, guidance, or technology.

14.2 Updates will be communicated to all staff, governors, and relevant third parties.

15 References

- **UK GDPR** and **Data Protection Act 2018**
- **Data Use and Access Agreement (DUAA)**
- **DfE Cyber Security Standards for Schools and Colleges (2023/2024)**
- **NCSC Cyber Security Guidance for Schools (2024)**
- **ICO Security Outcomes Guidance (2024)**

Version: October 2025
Approved by: *(Headteacher/Governing Body)*
Next Review Due: October 2026