ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Cyber Security

Risk Assessment & Awareness

This is part of a suite of policies for safeguarding children. Please also see our Child Protection and Safeguarding Policy for more.

Approved by:	David Preston, Headteacher & Director	**Date:**	01.09.25
	Di Gardiner, Safeguarding Director		
	Laura Sweetman, DSL & Head of School		
	Wynford Dore, Chair of the Board		
	Gareth Newman, Proprietor & Director		
	Rosie Sayers, Director		
	Geraint Newman, Director		
	Sanj Dhadda, Commercial Director		
Last Reviewed:	1st August 2025	**Review Period**	Annually
Next Review Due:	1st September 2026		

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

INTRODUCTION

Arnold Lodge School recognises its responsibility under the Department for Education's Digital and Technology Standards and the requirements set out in Keeping Children Safe in Education (KCSIE) 2025. UK schools and colleges must conduct an annual cyber risk assessment to identify vulnerabilities, assess threats, and ensure appropriate security measures are in place to protect pupils, staff, and data.

This assessment is also essential for insurance purposes, as some insurers will not cover cyber attacks if these requirements are not met.

Key Legislative and Regulatory Requirements

- Keeping Children Safe in Education (KCSIE) 2025 - Paragraphs 140-147
- Digital and Technology Standards (updated March 2025)
- UK GDPR and Data Protection Act 2018
- Management of Health & Safety at Work Regulations 1999
- Computer Misuse Act 1990

UNDERSTANDING CYBER SECURITY: THE ALS CONTEXT

Why Cyber Security Matters at Arnold Lodge School

Cyber security is not simply an IT issue—it is fundamentally a safeguarding issue. At Arnold Lodge School, we understand that cyber security sits at the intersection of child protection, data privacy, operational continuity, and educational excellence. A cyber incident can have profound and lasting impacts on our pupils, staff, families, and the wider school community.

The Threat Landscape for UK Schools

- Schools are increasingly targeted
- Educational institutions hold valuable personal data about children and families, making them attractive targets for cybercriminals. The education sector has seen a significant rise in cyber attacks, with ransomware attacks on schools increasing by over 50% in recent years. These attacks can:
    - Lock schools out of critical systems for days or weeks
    - Expose sensitive pupil and staff data
    - Disrupt learning and examinations
    - Cost tens of thousands of pounds to remediate
    - Damage reputation and trust with families

Recent high-profile attacks on UK schools have resulted in:

- Personal data of thousands of pupils and families stolen and published online
- Entire school networks encrypted by ransomware, forcing school closures
- Examination data lost during critical assessment periods
- SEND support plans and safeguarding records made inaccessible
- Insurance claims denied due to inadequate cyber security measures

According to the National Cyber Security Centre (NCSC):

- Educational institutions face an average of 1,000+ cyber attacks per week
- 60% of schools have experienced some form of cyber incident
- The average cost of a cyber attack on a UK school is £27,000-£50,000
- Recovery can take weeks or months, significantly disrupting education

Cyber Security as a Safeguarding Issue

At ALS, we recognise that cyber security failures directly impact child welfare and safety:

A data breach could expose:

- Safeguarding records and child protection concerns
- SEND assessments and medical information
- Contact details of vulnerable families
- Addresses of pupils with protection orders
- Information that could be used to target or harm children

Operational disruption affects vulnerable pupils. Many of our pupils rely on:

- Daily routines and structure that cyber incidents disrupt
- Electronic medical records for emergency care
- Communication tools to stay connected with support staff
- Assistive technologies that may be compromised

Cyber security failures can:

- Disable filtering and monitoring systems, exposing pupils to harmful content
- Allow unauthorised access to pupils' online activities and communications
- Compromise incident reporting systems like Whisper
- Expose pupils' personal information to predators or bullies

Cyber security is about staff knowledge and actions as much as about the software and hardware protections. Research shows that:

- 95% of cyber security breaches involve human error
- Phishing emails are the entry point for 80% of ransomware attacks
- Weak or reused passwords are exploited in 61% of data breaches
- Social engineering targets people, not technology

At ALS, we recognise that every staff member is part of our cyber security defence. A single click on a malicious link, a weak password, or an unencrypted laptop left in a car can undermine even the most sophisticated technical controls. This is why training, awareness, and a culture of vigilance are as important as firewalls and antivirus software.

The ALS-Specific Context

Arnold Lodge School faces specific cybersecurity challenges that inform this risk assessment:

1. **All-through setting with diverse age groups (EYFS to Sixth Form)**
   - Wide range of digital maturity and online risks
   - Different levels of device access and autonomy
   - Potential for older pupils to influence younger pupils online
   - Complex filtering and monitoring needs across age ranges

2. **Pupils with SEND and additional vulnerabilities**
   - Some pupils may be more susceptible to online manipulation
   - May find it harder to identify phishing, scams, or dangerous content
   - Require tailored cyber security and online safety education
   - Hold sensitive medical and support data requiring extra protection

3. **Parental engagement variations**
   - Some families highly engaged in online safety; others less so
   - Working parents may have limited time to monitor children's online activity
   - Some pupils may have largely unmonitored access to multiple platforms at home
   - School has limited control over home cyber security practices

4. **BYOD policy for Seniors**
   - Seniors with access to devices (in lessons)
   - 4G/5G could bypasses school filtering and monitoring systems
   - Requires trust in pupils' digital judgment and responsibility
   - Higher risk of exposure to inappropriate or extremist content

5. **Integration with Prevent strategy**
   - Online radicalisation is a recognised risk in our local context
   - Gaming platforms, message boards, and social media used for radicalisation
   - "Youth-on-youth" radicalisation through online peer interactions
   - Cyber security controls are essential for Prevent compliance

6. Dependence on IT provider

- Network management and security outsourced to third-party
- Need for clear accountability and strong SLAs
- Critical that provider understands education sector threats
- Must ensure provider meets required security standards

7. Small school with limited in-house IT expertise

- No dedicated in-house IT security specialist
- Reliance on external expertise and support
- Budget constraints for cyber security investments
- Need to prioritise cost-effective controls

Our Commitment

Arnold Lodge School is committed to:

- **Protecting our pupils** from cyber threats that could expose them to harm, disrupt their education, or compromise their personal information
- **Maintaining continuity of education** by ensuring our systems are resilient and recoverable
- **Safeguarding staff** by providing training, clear procedures, and a supportive culture where concerns can be raised
- **Meeting all regulatory requirements** including DfE standards, KCSIE, GDPR, and Prevent duty obligations
- **Being prepared** with robust incident response and business continuity plans
- **Learning and improving** through annual reviews, lessons from incidents, and staying informed of emerging threats
- **Integrating cyber security with safeguarding** so that technology protects rather than endangers our pupils

This annual cyber risk assessment is a critical tool in fulfilling these commitments. It identifies where we are strong, where we are vulnerable, and what actions we must take to protect our school community.

STATEMENT OF INTENT

Arnold Lodge School will:

- Conduct an annual cyber risk assessment
- Create and maintain a cyber awareness plan
- Secure digital technology and data effectively
- Ensure all staff and at least one governor complete annual cybersecurity training
- Review filtering and monitoring provision at least annually
- Maintain appropriate cyber security controls that support safeguarding duties

Cyber security is about staff behaviour and understanding as much as about the software and hardware protections.

The annual cyber risk assessment review team comprises:

- **DSL (Designated Safeguarding Lead):** Laura Sweetman - overall responsibility
- **Director:** Sanj Dhadda - strategic oversight
- **IT Provider/Manager:** TELFORD
- **Headteacher:** Dai Preston

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Cyber Risk Assessment: 2025-2026

LEADERSHIP AND GOVERNANCE

Hazard	Who is at risk?	Actions in place	Owner	Risk	Additional notes / next steps
Leadership team unaware of cyber security responsibilities and DfE requirements	Pupils, staff, Directors	> DSL has overall responsibility for cyber security standards > All Directors have read child protection policy and KCSIE 2025 > Dedicated Safeguarding Director (Di Gardiner) oversees compliance > Di has completed DSL training and is an ISI Reporting Inspector > Cyber security is a standing item on governance meetings	DSL, Safeguarding Director	Low	> Refresh leadership team annually on responsibilities > Ensure new SLT members receive cyber security briefing
Cyber security risks not given proper consideration by the board of directors	Strategic oversight gap	> Annual penetration test by Telford > Cyber security report an annual input to the directors	Head, Safeguarding Director	Medium	**PRIORITY ACTION:** Send Telford report to board on an annual basis Integrate cyber Secuirty reporting to DSL Termly Report
Insufficient strategic oversight of cyber risks	Pupils, staff, school operations	> Annual cyber risk assessment conducted > Board of Directors reviews cyber security compliance termly > Budget allocated for cyber security improvements	Safeguarding Director, Head	Medium	> Establish regular governance reporting cycle > Consider appointing specific governor with cyber security brief > Ensure cyber security in school development plan

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk	Additional notes / next steps
		> Incident response plan in place [to be developed in line with KCSIE 2026]			> Link cyber risks to financial and reputational risks
Inadequate budget for maintaining cyber security	Systems become outdated, increased risk	> IT budget is over £100,000 providing for ample funds to support > Cyber Security insurance is in place and confirmed	Head, Commercial Director	Medium	> School understands that financial cost of recovering from a Major Cybersecurity Budget appropriately to keep cyber related risk to a minimum > Include in annual budget cycle: Hardware refresh/replacement, Software licenses and updates, Training, Cyber insurance, Security tools and services, Incident response capabilities
Lack of integration between safeguarding and cyber security	Pupils, staff	> Cyber security explicitly referenced in safeguarding policy > DSL leads both safeguarding and cyber security compliance > Regular liaison between safeguarding team and IT provider	DSL	Low	> Continue integrated approach > Ensure all safeguarding staff understand cyber dimensions > Include cyber security in safeguarding audits
Cyber security policy does not exist or is outdated	Unclear expectations, compliance gap	> This cyber Security Risk Assessment contains the Policy work > In addition, ALS has: o Online Safety Policy o AI Policy	Head, IT Manager	**Low**	> Develop/review Cybersecurity Policy covering: Scope, Physical security, Asset management, User accounts, Devices, Data security, File sharing, Training, System security, Incident response, Budget commitment > Approve at Board November 2025 > Communicate to all staff > Review annually

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

2. TRAINING AND CAPABILITY

Hazard	Who is at risk?	Actions in place	Owner	Risk	Additional notes / next steps
Staff lack awareness of cyber security threats and responsibilities	Pupils, staff, school data	• All staff complete annual cybersecurity training • NCSC training pack used • Training delivered as part of: Annual Safeguarding Training [all staff - September], Individual Safeguarding Induction [mid-year joiners], Online safety modules via Educare • Regular Cybersecurity training integrated into Inset days • Staff briefings include cyber security updates	DSL, Heads of School, LB - induction lead	Medium	• Update training materials annually • Track completion rates • Include practical scenarios • the Key cyber security training • More specialist training for IT-responsible staff
"Blame culture" prevents reporting of security incidents	Incidents unreported, hidden vulnerabilities	• ALS promotes "No Blame" culture towards individuals who may fall victim to sophisticated scams • Focus on learning and improvement • Whistleblowing policy promoted	DSL, Head, SLT	Medium	• Regularly reinforce no-blame approach • Celebrate reporting of incidents • Use incidents as learning opportunities • Anonymous reporting options available
At least one governor has not completed annual cyber security training	Governance oversight weakened	• Safeguarding Director (Di Gardiner) has completed DSL and cyber security training • Governor training records maintained	Safeguarding Director, Board	Low	• Ensure compliance checked annually • Provide refresher training • Brief all governors on cyber risks termly
Staff unable to recognise phishing, social engineering,	Pupils, staff, data security	• Regular staff briefings on current threats • Email security awareness included in training • Examples of phishing attempts shared in staff bulletins	IT Manager, DSL	High	• Consider implementing phishing simulation exercises (e.g. Sophos Phish or LGfL tool)

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk	Additional notes / next steps
or other cyber threats		• Reporting mechanism for suspicious emails • Users required to check with sender via alternative method if email seems suspicious			• Link to training material for staff who click • Increase frequency of threat updates • Share real examples (anonymized) • Practical exercises in Inset
Insufficient understanding of online platforms pupils use	Safeguarding, radicalisation risks	• Training on key indicators from online perspective • Staff attend assemblies/briefings on dangers • Updates from local Prevent Officer (Geoff Thomas)	Online Safety Lead, DSL	Medium	• Annual review of staff confidence in identifying online risks • Specific training on emerging platforms • Gaming platform awareness • Social media trend updates
Staff with IT system responsibilities lack specialist cybersecurity training	System vulnerabilities, poor security design	• IT provider maintains systems. DW, in-house IT, has appropriate training.	IT Manager, Head	Medium	• Provide more specialist training to staff responsible for maintaining IT systems • Ensure IT provider staff are appropriately qualified • Regular security awareness updates for technical staff • Professional development in cyber security

3. ASSET INVENTORY AND SYSTEM SECURITY

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Incomplete asset inventory leading to unmanaged devices	Data security, network integrity	• IT asset register maintained • All school devices logged and tracked • Regular audits of hardware and software	IT Manager	Medium	PRIORITY ACTION: • Conduct full asset audit by [date] • Maintain registers for: Physical devices (servers, switches, desktops, laptops), Files/systems holding confidential data, Network hardware • Include cloud services and third-party systems • Document all critical systems
Server/communications room inadequately secured	Network infrastructure, all systems	• Securely locked away • DW works within the server room.	IT Manager, Operations Manager	Medium	• Review physical security of server/comms room • Ensure lockable secure location • Appropriate environmental controls • Access log for server room • Limit access to authorised personnel only

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Network hardware reaching end-of-life without security support	Network vulnerability, all systems	• Upkept by Telford DW working on asset plan for updating laptops and hardware	IT Manager	Medium	• Create asset lifecycle plan • Pro-actively plan for replacement of network hardware, operating systems and software before vendors stop providing security support • Budget for hardware refresh cycle
Outdated or unpatched systems vulnerable to attack	All users, school data	• Automatic updates enabled where possible • Regular patch management schedule • IT provider monitors security updates	IT Manager	Medium	• Document comprehensive patch management policy • Include network hardware patching schedule • Operating systems security patching • Software security patching • Test updates before deployment • Track patching compliance
Weak password policies	User accounts, sensitive data	• Password complexity requirements in place • Staff guidance on strong passwords • Regular password change reminders	IT Manager, DSL	Medium	• Implement multi-factor authentication (MFA) for: All administrative accounts, Where practicable for standard users • Enforce minimum password standards • Consider password manager recommendation

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					• Clear password policy documentation
User accounts compromised (phishing, credential theft)	Individual users, wider network	• Staff training on phishing recognition • Users must change passwords if credentials suspected compromised • Users must inform IT Support immediately • Personal accounts not used for work purposes	IT Manager, DSL	High	• Implement MFA as primary defence • Consider phishing simulation exercises • Clear incident reporting procedure • Account monitoring for suspicious activity
Excessive administrative accounts	Privilege escalation risk	DW to undertake review of key systems and identify where multiple administrative accounts exist	IT Manager	Medium	• Maintain minimal administrative accounts • Regular review of admin privileges • Remove admin rights when staff leave • Document justification for each admin account
Insufficient network security controls	Network access, data security	• School network has firewall protection • Separate guest Wi-Fi network • Network monitoring by IT provider	IT Manager	Low to Medium	• Review firewall configuration annually • Document network segmentation • Segregate wireless networks for visitors & staff personal devices from school systems • Consider enhanced

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					monitoring • Active management of client firewalls on devices
Inadequate backup and recovery procedures	Data loss, operational continuity	Back up plan to be created IT manager has created back up drives for key information Key systems held on the cloud (iSams; Xero; MyConceron; OneDrive)	IT Manager, Head	CRITICAL	PRIORITY ACTION: • Document full backup strategy following 3-2-1 methodology: 3 versions of data, 2 different types of media, 1 copy offsite/offline • Test restoration procedures regularly • Ensure backups stored offline/offsite • Actively manage and test backups • Consider Gridstore or similar for online backup • Document which backups need restoring first for school to become operational (system impact assessment)
Backups not protected from ransomware	Ransomware could encrypt backups	• [Are backups air-gapped or immutable?] • [Offline backups maintained?]	IT Manager	TO BE ASSESSED	• Ensure at least one backup copy is offline/offsite • Backups not accessible from network • Immutable backups where possible • Regular testing that

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					backups are uncompromised
Physical security of devices insufficient	Device theft, data breach	• CCTV coverage of site • Reception access control • Devices stored securely when not in use • Users required to lock devices when left unattended	Operations Manager, IT Manager	Low to Medium	• Review device security protocols • Ensure encryption on portable devices • Clear desk policy • Enforce device locking when unattended • Lockable cabinets for equipment
Devices not configured with minimum security controls	Compromise of individual devices, lateral network attack	• [Document current device security configuration]	IT Manager	TO BE ASSESSED	Ensure all devices configured with minimum controls: • Password protection • Full disk encryption • Client firewalls enabled • Anti-virus / malware software (e.g. Sophos, Malwarebytes) • Automatic security updates enabled • Removal of unrequired and unsupported software • Autorun disabled on removable media • Minimal administrative accounts

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Software no longer supported by vendors	Unpatched vulnerabilities	• [Inventory of all software and support status]	IT Manager	TO BE ASSESSED	• Create software inventory with vendor support end dates • Pro-actively plan for replacement before support ends • Budget for software upgrades/replacements • Remove unsupported software from network
Lost or stolen devices not reported quickly	Extended window for data breach	• Users required to report lost/stolen equipment ASAP to IT Support • Users required to change all account passwords immediately • Device tracking/remote wipe capability [confirm]	IT Manager, All Staff	Medium	• Clear and simple reporting procedure • Ensure all mobile devices have remote wipe capability • Staff training on reporting requirements • Out-of-hours contact for urgent reports

4. FILTERING AND MONITORING (Annual Review Required)

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Inadequate filtering allowing access to harmful content	Pupils, safeguarding	• School IT network has appropriate filters • Filters block harmful and inappropriate content • Content categories blocked include: Child sexual abuse content, Terrorist content, Extremist material, Sexual content, Violence and hate speech • Filtering does not unreasonably impact teaching and learning	IT Manager, DSL	Medium	ANNUAL REVIEW COMPLETED: [Date] • Check filter effectiveness • Review content categories • Test access to educational resources • Review students' browsing history sample
Insufficient monitoring of online activity	Pupils, safeguarding concerns	• School email accounts monitored by IT staff • Monitoring strategies in place that meet safeguarding needs • Alerts configured for concerning searches/content • DSL notified of safeguarding concerns	IT Manager, DSL	Medium	• Document monitoring procedures • Clarify alert triggers • Review escalation process • Consider keywords for alerts
Filtering and monitoring not reviewed annually	Compliance failure, insurance risk	• Formal annual review scheduled • Review team: Governor, SLT member, DSL, IT provider • Review recorded and shared appropriately • Tools used: 360 safe and/or LGfL online safety audit	DSL, Review Team	CRITICAL	ANNUAL REVIEW DUE: September 2026 • Schedule review meeting • Use DfE self-assessment tool • Document findings and actions
Personal devices bypass school filtering (Years 12-13)	Pupils in Sixth Form accessing inappropriate content	• Personal devices are not allowed for pupils up to Year 11 • Years 12-13 may use personal devices with 4G/5G access • Sixth Form pupils receive specific online safety education • Acceptable use policy for Sixth Form devices	Head of Sixth Form, DSL	Medium to High	• Review Sixth Form device policy • Consider additional controls or monitoring • Parental engagement for Sixth Form

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					• Emphasise responsible use expectations

5. ONLINE SAFETY AND SAFEGUARDING INTEGRATION

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Pupils exposed to harmful content online (4Cs: Content, Contact, Conduct, Commerce)	Pupils	• Online safety policy reflects 4Cs framework • Pupils taught how to stay safe online via ICT curriculum, PSHEE, assemblies • Whisper reporting mechanism for inappropriate conduct • Mobile device policy up to Year 11	DSL, PSHEE Lead, ICT Teacher	Medium	• Annual review of online safety provision • Use UKCIS audit tools
Pupils access extremist or radicalising content	Pupils, prevent duty compliance	• Filtering blocks terrorist and extremist content • Staff trained to recognise signs of radicalisation • Clear referral route through DSL to Channel • Integration with Prevent risk assessment	DSL, Prevent Lead	Medium	• Cross-reference with Prevent Risk Assessment • Monitor for concerning online behaviour
Cyberbullying and online harassment	Pupils, wellbeing	• Clear behaviour policy on cyberbullying • Zero tolerance approach to discriminatory behaviour • Staff respond to witnessed harassment • Pupils encouraged to report and challenge	DSL, Heads of Key Stage	Medium	• Regular pupil surveys on online experiences • Parent workshops on cyberbullying

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Pupils sharing inappropriate images (consensual/non-consensual)	Pupils, safeguarding, legal	• KCSIE guidance on sharing nudes and semi-nudes followed • Education on consequences and risks • Clear reporting and response procedures • Police liaison when appropriate	DSL	High	• Specific training for staff

6. DATA PROTECTION AND PRIVACY

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Confidential data not properly identified and classified	Data security, GDPR compliance	• School defines confidential data as: - Personally identifiable information (as per ICO) - Special category personal data (as per ICO) - Unpublished financial information - Safeguarding records - SEND assessments • Data classification guidance in Data Protection Policy	DPO/Head, DSL	Medium	• Review and update confidential data definitions • Staff training on data classification • Label sensitive files appropriately • Regular audits of data handling
Data breach exposing personal information	Pupils, staff, parents, GDPR compliance	• Data protection policy in place • Staff trained on GDPR requirements • DPO appointed: Helen King • Access controls on sensitive data • Privacy notices issued • Breach reporting procedures documented	DPO (Helen King), DSL	**High**	• Review data protection policies annually • Conduct data mapping exercise • Document data processing activities • 72-hour breach reporting to ICO procedures clear • Breach notification templates ready

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Unauthorised access to pupil/staff data	Data subjects, legal liability	• User access controls based on role • Passwords required • Staff leave process includes access removal • MIS system security reviewed	IT Manager (Telford), Operations Manager	**Medium to High**	• Implement MFA for admin accounts • Regular access audits (quarterly) • Document access logs • Principle of least privilege enforced
Files shared insecurely (email, unencrypted)	Data breach, interception	• Staff guidance on secure file sharing • Users required to: - Consider if email could be phishing - Keep school files on school systems - Not send school files to personal accounts - Verify recipient before sending - Use file encryption where possible - Alert IT Support/DPO to breaches or scams	IT Manager (Telford), DSL, DPO	**High**	• Implement secure file sharing solution • Email encryption for sensitive data • Clear policy on acceptable file sharing methods • Regular reminders to staff • Monitor for data sent to personal accounts
Confidential data stored inappropriately (USB drives, personal devices, unencrypted laptops)	Data loss, theft, breach	• Policy that school files should remain on school systems • Full disk encryption [to be confirmed on all devices] • USB/removable media not accepted on school devices (disabled)	IT Manager (Telford), DSL	**High**	PRIORITY ACTION: • Ensure full disk encryption on all laptops • Policy on removable media usage • Encrypted USB drives if needed • Regular checks of where data is stored • Data loss prevention tools if feasible
Insecure data sharing with third parties	Data security, compliance	• Data processing agreements with third-party providers • Vendor security assessments conducted • Due diligence on cloud services	Head, IT Manager (Telford)	Medium	• Review all third-party contracts for data clauses • Maintain supplier security register • Annual vendor security reviews • Document data flows to/from third parties • Ensure Article 28 GDPR contracts in place
Data not encrypted on portable devices	Data loss in theft/loss scenarios	• [Current encryption status to be documented] • Full disk encryption required	IT Manager (Telford)	**TO BE ASSESSED**	• Implement full disk encryption on all laptops and portable devices • Policy on removable media

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					• Remote wipe capability for mobile devices • Audit encryption compliance
Inadequate secure disposal of data/devices	Data recovery by unauthorised parties	• IT provider manages device disposal • Hard drives wiped/destroyed • Certificate of destruction obtained	IT Manager (Telford)	Low to Medium	• Document disposal procedures • Audit trail for disposed equipment • Secure paper shredding for printed confidential data • Verify disposal certificates received
Data retention periods not followed	GDPR non-compliance, excessive data storage	• [Document retention schedule in place?] • [Regular deletion of out-of-date data?]	DPO (Helen King), IT Manager (Telford)	Medium	• Create/review data retention schedule • Automated deletion where possible • Annual data cleansing exercise • Document destruction logs
Subject access requests not handled securely	Data breach in response process	• SAR procedures in Data Protection Policy • DSL/DPO manages requests	DSL, DPO (Helen King)	Low to Medium	• Ensure SAR responses sent securely • Verify identity before releasing data • Redact third-party information appropriately • Track and log all SARs

7. INCIDENT RESPONSE AND BUSINESS CONTINUITY

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
No cyber incident response plan	Delayed response, increased damage	• [Document if incident response plan exists] • [Key contacts identified?] • [Reporting procedures clear?]	DSL, Head, IT Manager (Telford)	**CRITICAL**	**PRIORITY ACTION:** **• Develop Cybersecurity Major Incident Response Plan including:** **- Key decision-makers** **- System impact assessments and**

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					restoration priorities - Emergency plans to function without access to systems/data - Alternative communication methods - Emergency budgets and access procedures - Key agencies for support • Integrate with safeguarding procedures • Regularly test the plan
Staff unclear on incident reporting	Delayed detection, poor response	• Clear reporting procedures in safeguarding policy • Staff can contact DSL, DDSL, Head • IT support contact details known • Users required to report suspected threats or security weaknesses to Risk Register Owner	DSL, IT Manager (Telford)	Medium	• Create simple cyber incident reporting flowchart • Include in staff handbook • Regular reminders in briefings • Clear escalation process • Out-of-hours contact details
Critical systems not identified with restoration priorities	Poor recovery decisions, extended downtime	• [Have critical systems been documented?] • [Restoration priority order clear?] • [Which backups need restoring first for school to become operational?]	Head, IT Manager (Telford), SLT	**TO BE ASSESSED**	**PRIORITY ACTION: • Conduct system impact assessment • Rank systems by criticality: 1. Safeguarding systems (e.g. MyConcern) 2. Learning platforms 3. MIS systems 4. Communication systems 5. Administrative systems • Document RTO (Recovery Time Objective) for each • Document RPO (Recovery Point Objective) for each**

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
No emergency communication methods if systems down	Cannot coordinate response	• [Alternative communication methods identified?] • [Copies of contact details stored offline?] • [Staff personal contact details available?]	Head, Operations Manager	**TO BE ASSESSED**	• Printed contact lists kept in secure locations • Alternative communication methods (e.g. personal phones, WhatsApp groups) • Pre-prepared communication templates • Cascade communication plan
Emergency budget not accessible during incident	Cannot procure urgent support	• [Emergency budget identified?] • [Who can access it and how?] • [Process documented?]	Head, Commercial Director (Sanj Dhadda)	**TO BE ASSESSED**	• Define emergency cyber incident budget • Document authorization process • Ensure rapid access for urgent costs • Pre-approved vendors/contractors
Ransomware attack encrypts school data	All operations, data access, potential school closure	• Antivirus software on all devices • Staff training on phishing recognition • Backup systems in place [to be documented] • User account security measures • Cyber insurance in place	IT Manager (Telford), DSL	**High**	**Critical controls:** • Review ransomware protection • Ensure backups offline/offsite • Test backup restoration • Establish no-pay policy • Cyber insurance review • Incident response plan specific to ransomware • Know who to contact (NCSC, police, ICO)
Malware infection spreads across network	Multiple systems compromised	• Anti-virus / malware software on devices • Active management of anti-virus systems • Automatic security updates • Network segmentation [to be enhanced]	IT Manager (Telford)	**High**	• Ensure comprehensive endpoint protection • Network segmentation to limit spread • Isolate infected devices quickly • Regular scans and active monitoring • Incident response procedures for malware
DDoS attack overwhelms internet connection	Loss of internet access, systems unavailable	• [DDoS protection in place?] • [ISP provides mitigation?]	IT Manager (Telford)	Low to Medium	• Review with ISP DDoS protection options • Understand school's internet dependency

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					• Alternative connectivity options • Communication plan if internet down
Inadequate business continuity planning	School operations, pupil learning, extended closure	• Remote learning capability exists (see Online Safety Policy) • [Alternative arrangements for key systems?] • [Manual workarounds documented?]	Head, SLT	**CRITICAL**	**PRIORITY ACTION:** **• Develop cyber-specific BC plan** **• Identify critical systems and RTOs** **• Test recovery procedures annually** **• Document manual workarounds for key processes** **• Remote learning contingency** **• Paper-based alternatives for registers, safeguarding logs** **• Financial system alternatives**
Cyber incident response never tested	Untested plans may fail when needed	• Annual penetration testing by Telford conducted • [Incident response plan tested?] • [When was last test/simulation?]	Head, IT Manager (Telford), DSL	**TO BE ASSESSED**	**PRIORITY ACTION:** **• Schedule annual cyber incident simulation** **• Tabletop exercise with key staff** **• Test backup restoration** **• Test communication methods** **• Review and update plans based on learning** **• Document lessons learned**
No relationship with key support agencies	Delayed external support	• IT provider (Telford) contracted • Cyber insurance in place • [Other key agencies identified?]	Head, IT Manager (Telford)	Medium	• Document all key external contacts: - IT support company (Telford) - NCSC CareCERT - Local police cyber crime unit - Action Fraud - ICO - Cyber insurance provider

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					- DfE regional team • Pre-register where possible

8. THIRD-PARTY AND SUPPLIER RISKS

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
IT provider/contractor cyber security insufficient	School network, data	• IT provider (Telford) contracted for network management • Annual penetration testing conducted • [Provider security standards documented?] • [SLAs include cyber security requirements?] • IT Support builds security principles into design of IT services	Head, Operations Manager, Commercial Director (Sanj Dhadda)	**Medium to High**	**PRIORITY ACTION:** **• Review IT provider (Telford) contracts** **• Obtain provider's cyber security certifications** **• Document provider responsibilities including:** **- Security patching schedules** **- Active anti-virus management** **- Backup management and testing** **- Security controls review** **- New system security risk reviews** **• Include incident notification clauses** **• Define response time SLAs for security incidents**
IT provider does not actively manage security	Vulnerabilities accumulate	• IT provider (Telford) contracted for security management • Annual penetration testing • [Regular security reviews conducted?] • [Patching schedules documented?]	IT Manager (Telford)	Medium	• Ensure IT Support (Telford) actively manages: - Anti-virus systems - Security patching - Regular review/update of security controls • Request quarterly security reports • Regular meetings to review security posture

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Cloud service providers experience breach	School data, third-party hosted	• Major providers used (assume reasonable security) • [List key cloud services] • [Data processing agreements in place?] • [Provider security certifications verified?]	IT Manager (Telford), Head	Medium	• Inventory all cloud services: - MIS systems - Learning platforms - Email/communication tools - File storage - Backup services • Review DPAs and security measures • Verify ISO 27001 or equivalent certifications • Understand provider incident notification process • Review where data is stored geographically
Supply chain attack via compromised software	Network security, data	• Software downloaded from official sources only • Updates from verified providers • IT provider vets software installations • Removal of unrequired and unsupported software	IT Manager (Telford)	Medium	• Policy on software installation (admin rights required) • Approved software list maintained • Regular software audits • Verify software sources • Monitor for vendor security advisories
Suppliers/contractors with remote network access	Unauthorized access, backdoor entry	• [Document suppliers with remote access] • [Access controls and monitoring in place?] • [MFA required for remote access?]	IT Manager (Telford)	**Medium to High**	• Inventory all remote access accounts • MFA required for all remote access • Time-limited access where possible • Regular access reviews • Monitor remote access logs • Remove access when contract ends
Visiting contractors with physical network access	Network security	• Visitors never left alone with pupils • Visitor procedures in place • All visitors signed in and accompanied • [Network access controls for contractors?]	Operations Manager, IT Manager (Telford)	Low to Medium	• Document contractor network access policy • Separate contractor Wi-Fi if needed • Access limited to necessary systems • No access to school domain without

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					authorization • Supervised at all times
Third-party software vulnerabilities exploited	Data breach, system compromise	• IT provider (Telford) monitors security updates • [Process for third-party software patching?] • [Regular updates applied?]	IT Manager (Telford)	Medium	• Ensure third-party software included in patch management • Subscribe to vendor security advisories • Test and apply security patches promptly • Understand vendor patch release cycles
Vendor going out of business leaves systems unsupported	Loss of support, unpatched vulnerabilities	• [Financial stability of key vendors checked?] • [Contingency plans for vendor failure?]	Head, IT Manager (Telford)	Low to Medium	• Monitor key vendor stability • Ensure data portability in contracts • Identify alternative suppliers for critical systems • Data extraction procedures documented

9. PHYSICAL SECURITY AND ACCESS CONTROL

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Unauthorised physical access to IT systems	Network security, data	• Secure site with reception access control • CCTV coverage including IT areas • Server room secured [confirm location and access controls] • All visitors signed in and accompanied	Operations Manager	Low	• Review server room security • Limit access to authorised personnel • Audit access logs • Environmental controls verified (air conditioning, fire suppression)
Unlocked workstations allow	User accounts, data	• Clear desk policy [to be confirmed] • Staff guidance on locking computers • Auto-lock after inactivity [confirm settings]	IT Manager (Telford), DSL	Medium	• Implement/enforce clear desk policy • Reduce auto-lock timeout to 5-10 minutes

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
unauthorised access					• Regular spot checks • Staff reminders in briefings
Lost or stolen devices containing school data	Data breach	• Device tracking/remote wipe capability [confirm] • Devices reported lost immediately • Personal devices policy for Sixth Form • Full disk encryption [to be confirmed]	IT Manager (Telford), Staff	Medium	• Ensure all mobile devices have remote wipe • Clear reporting procedure • Staff training on immediate reporting • Review insurance coverage for lost devices

10. EMERGING TECHNOLOGIES AND SPECIAL CONSIDERATIONS

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
Generative AI tools (e.g. ChatGPT) create cyber security or safeguarding risks	Pupils, data privacy	• DfE guidance on Generative AI reviewed • Comprehensive AI Policy in place • Filtering and monitoring apply to AI tools • Staff guidance on appropriate AI use • Pupil education on AI safety and privacy • Approved AI tools list maintained (see AI Policy) • Risk assessments required for new AI tools	DSL, SLT, AI Lead (Headteacher)	Medium	• Monitor emerging AI risks • Review AI Policy annually • Consider data privacy implications of AI tool use • Review DfE product safety expectations • Staff training on AI risks and appropriate use • Integration with Online Safety education
AI tools used to input confidential data inappropriately	Data breach, GDPR violation	• AI Policy prohibits entering personal/confidential data into open AI tools • Staff training on data protection with AI	DPO (Helen King), AI Lead (Headteacher)	**High**	• Regular reminders to staff about AI data protection • Monitor for policy breaches • Clear consequences for data protection violations • Consider technical controls to

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
		• Only approved AI tools may be used • DPO oversight of AI usage			prevent data entry into unapproved tools
Deepfakes and AI-generated content used to bully or harass pupils	Pupils, safeguarding	• Online Safety Policy addresses deepfakes • AI Policy treats AI bullying seriously • Zero tolerance approach in Behaviour Policy • Pupils educated about deepfakes (PSHEE, assemblies) • Staff trained to recognise AI-generated harmful content	DSL, AI Lead (Headteacher)	**Medium to High**	• Continue education on identifying deepfakes • Clear reporting mechanisms • Swift response to incidents • Liaison with police for serious cases
Internet of Things (IoT) devices on network	Network security	• [Document IoT devices: smart boards, security cameras, etc.] • [Are IoT devices on separate network?] • [Default passwords changed?]	IT Manager (Telford)	**TO BE ASSESSED**	• Audit all IoT devices: - Interactive whiteboards - Security cameras/CCTV - Printers with network connectivity - Door entry systems - Any "smart" devices • Change default passwords on all IoT devices • Consider network segmentation for IoT • Regular firmware updates • Document all IoT devices in asset register
BYOD (Bring Your Own Device) in Sixth Form	Data security, filtering bypass	• Personal devices allowed Years 12-13 • Acceptable use policy in place • Education on responsible use • Devices not connected to school network for data access	Head of Sixth Form, DSL	**Medium to High**	• Review BYOD policy annually • Consider whether BYOD devices should access school systems • Enhanced online safety education for Sixth Form

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
		• Enhanced online safety education for Sixth Form			• Parental engagement letters for Years 12-13 • Monitor for concerning online behaviour • Regular reminders about acceptable use
Online gaming platforms used for communication	Pupils, safeguarding, radicalisation	• Staff awareness of gaming platforms as radicalisation vector (per local Prevent Officer Geoff Thomas) • Education in PSHEE on gaming safety • Parental guidance on monitoring gaming • Integration with Prevent Risk Assessment	DSL, Prevent Lead (Kenny Owen), Online Safety Lead	**Medium to High**	• Specific training on gaming platforms • Youth-on-youth radicalisation risks via gaming • Parental workshops on gaming safety • Monitor for pupils discussing concerning gaming interactions • Cross-reference with Prevent concerns
Social media platforms constantly evolving with new risks	Pupils, online safety	• Regular updates to staff on emerging platforms • Pupils educated on social media risks • Monitoring of pupil discussions about new platforms • Online Safety Lead stays informed of trends	Online Safety Lead, DSL	Medium	• Quarterly updates to staff on new platforms • Include in Online Safety curriculum • Parental communications about emerging risks • Staff training on identifying new platform risks

11. SPECIFIC VULNERABILITIES: ALS CONTEXT

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
ALS pupils with SEND more vulnerable to online exploitation	Pupils with SEND	• Robust pastoral system • SEND and behaviour policies in place • Support from SLT, SENCo, parent liaison • Open, honest, supportive culture • Tailored online safety education where appropriate	SENCo, DSL, Heads of SEND	**Medium to High**	• Identify pupils most at risk of not understanding materials they may be accessing • Conversations with parents about online safety protocols • Personalised online safety education for vulnerable pupils • Enhanced monitoring where safeguarding concerns exist
ALS pupils vulnerable due to low parental engagement in online safety	Pupils at home	• Robust pastoral system • Frequent parental communications emphasising importance of parental monitoring • School advocates for open device policies at home • Parental workshops offered	DSL, Heads of School, Heads of KS	**Medium to High**	**• Identify pupils who have shared views counter to British values and discuss with parents whether there are more online safety protocols that can be put in place** **• Identify pupils with open access to multiple platforms due to limited parental oversight** **• Target support for at-risk families** **• Increase frequency of parental communications** **• Consider mandatory parental online safety sessions**
All-through setting: older pupils influence younger pupils online	Younger pupils, safeguarding	• Head of Sixth Form vigilant for extremist views • Education on peer responsibility • Clear behaviour expectations across age ranges • Youth-on-youth radicalisation awareness (per local Prevent Officer) • Age-appropriate separation of online spaces where possible	Head of Sixth Form, DSL, Heads of KS	Medium	• Monitor cross-age group online interactions • Education on positive digital citizenship for older pupils • Reporting mechanisms for concerning behaviour • Swift intervention when issues identified

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
					• Integration with Prevent Risk Assessment
ALS pupils accessing inappropriate online culture outside school	Pupils, Prevent risks	• Strong view of pupil culture within school • Recognition that online is highest risk area • Education through assemblies, mentor time, PSHEE • Whisper reporting mechanism • Integration with Prevent risk assessment • Proactive curriculum promoting British values	DSL, Online Safety Lead, Prevent Lead (Kenny Owen)	**Medium to High**	**PREVENT IN CONTEXT [ALS]** **• Continue proactive curriculum** **• Increase online safety emphasis** **• Parent workshops on online culture and radicalisation risks** **• Monitor for emerging platforms/risks** **• Specific focus on:** **- Gaming platforms** **- Message boards** **- Social media** **- Great Replacement narrative** **- Extreme right wing content** **- Islamist extremist content**
Small school with limited in-house IT expertise	All cyber security areas	• Reliance on external IT provider (Telford) • Annual penetration testing • IT budget over £100,000 • DSL has overall responsibility for cyber security • Board oversight of cyber risks	Head, DSL, Commercial Director (Sanj Dhadda)	Medium	• Ensure Telford contract includes all necessary security services • Consider cyber security training for at least one internal staff member • Maintain strong relationship with IT provider • Regular security review meetings • Ensure clear escalation procedures • Budget appropriately for external expertise
Dependence on IT provider (Telford)	Single point of failure	• Contract with Telford in place • Annual penetration testing • [SLAs documented?]	Head, Commercial Director (Sanj Dhadda)	Medium	• Review Telford contract and SLAs • Identify backup IT support provider for emergencies • Ensure knowledge transfer so school

Hazard	Who is at risk?	Actions in place	Owner	Risk Level	Additional notes / next steps
for all security functions		• [Response times agreed?] • [Backup provider identified?]			has some basic capability • Document all systems and configurations • Regular review meetings with Telford • Consider what happens if Telford unavailable
Budget constraints limit cyber security investments	Overall security posture	• IT budget over £100,000 providing ample funds • Cyber insurance in place • Board understands that prevention costs less than recovery • Annual budget allocation for cyber security	Head, Commercial Director (Sanj Dhadda), Board	Low	• Continue to budget appropriately • Prioritise cost-effective controls • Focus on high-impact, low-cost measures (training, policies, procedures) • Balance expensive technical controls with staff awareness • Multi-year planning for major investments
Local Prevent context: Online radicalisation risks in Warwickshire	Pupils, Prevent duty	• Integration with Prevent Risk Assessment • Staff training from local Prevent Officer (Geoff Thomas) • Awareness of local risks: - Islamist extremist groups (ISIS, Al Qaeda) - Extreme right wing terror groups (fastest growing nationally) - Great Replacement narrative - Local activism by extremist groups - Online exposure during pandemic - Youth-on-youth radicalisation • Filtering blocks extremist content • Clear referral route through DSL to Channel	DSL, Prevent Lead (Kenny Owen)	**Medium to High**	• Annual Prevent training including local context • Regular updates from Geoff Thomas (Prevent Officer) • Monitor for concerning online behaviour • Cross-reference with Cyber Risk Assessment • Parent communications about online radicalisation • Staff confidence in identifying extremist content online

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

RISK SUMMARY AND PRIORITY ACTIONS

Risk Level Summary

- **CRITICAL Risk Areas:** No cyber incident response plan, inadequate business continuity planning
- **HIGH Risk Areas:** Data breach exposures, ransomware threat, malware spread, file sharing insecurity, data storage on unencrypted devices, AI tool misuse with confidential data, BYOD Sixth Form, parental engagement gaps, SEND vulnerabilities, online radicalisation (local Prevent context)
- **MEDIUM Risk Areas:** Staff training consistency, IT provider dependency, third-party risks, physical security, backup documentation/testing, data retention, network security, emerging technologies
- **LOW Risk Areas:** Leadership awareness, governance oversight, budget adequacy, some operational controls

IMMEDIATE CRITICAL PRIORITIES (Complete within 1 month)

#	Priority Action	Owner	Why Critical
1	Develop Cybersecurity Major Incident Response Plan	DSL, Head, IT Manager (Telford)	No plan means chaotic response, extended downtime, and potential school closure. Required for insurance coverage.
2	Document and test backup procedures following 3-2-1 methodology	IT Manager (Telford), Head	Backups are last line of defense against ransomware. Must verify backups work and are offline/offsite.
3	Complete system impact assessment and restoration priorities	Head, IT Manager (Telford), SLT	Need to know which systems restore first for school to operate. Critical for incident response.
4	Ensure full disk encryption on all portable devices	IT Manager (Telford)	Protects data in theft/loss scenarios. GDPR requirement. Insurance requirement.
5	Implement secure file sharing procedures and email encryption	IT Manager (Telford), DSL, DPO (Helen King)	High risk of data breach through insecure email. Need immediate controls.

ARNOLD LODGE

4 - 18 yrs Co-educational Independent Day School

HIGH PRIORITIES (Complete within 3 months)

#	Priority Action	Owner	Rationale
6	Complete annual filtering and monitoring review	DSL and Review Team (Governor, SLT, IT provider)	DfE requirement. Insurance requirement. Safeguarding essential. Due September 2026.
7	Implement multi-factor authentication for admin accounts	IT Manager (Telford)	Primary defense against credential compromise. Industry best practice.
8	Review IT provider (Telford) contracts and security requirements	Head, Commercial Director (Sanj Dhadda)	Ensure clear security responsibilities, SLAs, and incident response procedures.
9	Develop cyber-specific Business Continuity Plan	Head, SLT	Need documented manual workarounds. Remote learning contingency. Paper-based alternatives.
10	Conduct full IT asset audit including cloud services	IT Manager (Telford)	Cannot protect what you don't know you have. Foundation for all other controls.
11	Review and strengthen Sixth Form BYOD policy	Head of Sixth Form, DSL	Highest risk group for exposure to harmful content. Bypasses filtering.
12	Implement phishing simulation exercises for staff	IT Manager (Telford), DSL	95% of breaches involve human error. Need to test and train staff.
13	Create emergency communication and budget procedures	Head, Operations Manager, Commercial Director (Sanj Dhadda)	Essential for coordinating incident response if systems down.

#	Priority Action	Owner	Rationale
14	Schedule and conduct cyber incident simulation exercise	Head, IT Manager (Telford), DSL	Test incident response plan. Identify gaps. Train key staff.
15	Deliver parental workshops on online safety and radicalisation	DSL, Online Safety Lead, Prevent Lead (Kenny Owen)	Address parental engagement gaps. High risk area for ALS pupils.

MEDIUM-TERM ACTIONS (Complete within 6 months)

16. Conduct comprehensive data protection audit and mapping exercise
17. Document all remote access accounts and implement MFA
18. Create data retention schedule and conduct annual data cleansing
19. Review all third-party contracts for data and security clauses
20. Audit all IoT devices and implement network segmentation
21. Enhanced training on gaming platforms and youth-on-youth radicalisation
22. Create hardware and software lifecycle/replacement plans
23. Implement/enforce clear desk policy with auto-lock settings
24. Document comprehensive patch management policy and schedule
25. Server/communications room physical security review
26. Inventory all cloud services with security certifications verified
27. Create simple cyber incident reporting flowchart for staff
28. Review cyber insurance coverage and ensure compliance with requirements
29. Establish quarterly security review meetings with Telford

30. Identify backup IT support provider for emergencies

ONGOING ACTIONS

31. Maintain staff training completion tracking
32. Regular threat intelligence updates to staff (at least termly)
33. Termly reports to Board of Directors on cyber security
34. Continuous improvement of parental communications on online safety
35. Integration with Prevent strategy and risk assessment
36. Annual policy reviews (Cybersecurity Policy, Data Protection, Online Safety, AI Policy)
37. Quarterly access rights audits
38. Regular monitoring of vendor security advisories
39. Active management of anti-virus and backup systems
40. Monthly staff briefings with cyber security updates
41. Maintain asset registers (update as changes occur)
42. Regular review and update of security controls
43. Monitor for concerning online behaviour patterns
44. Maintain relationships with key support agencies (NCSC, police, ICO, Telford, cyber insurance provider)
45. Annual penetration testing by Telford (already in place - continue)

NOTES

This cyber risk assessment should be read in conjunction with:

- ALS Risk Assessment Policy
- ALS Cybersecurity Policy

- ALS Online Safety Policy
- ALS AI Policy
- ALS Safeguarding Policy
- ALS Prevent Risk Assessment
- ALS Data Protection Policy
- KCSIE 2025

HEADTEACHER	
[Signature]	[Date]

DSL/PREVENT LEAD	
[Signature]	[Date]

DATE OF NEXT REVIEW:	[Date]

ARNOLD LODGE

RESPICE FINEM est.1864

4 - 18 yrs Co-educational Independent Day School