Title	OBR Cyber Security Policy
Operational Owner	Simon Clark
Executive Owner	Lynda Walker
Effective Date	October 2026
Review Date:	October 2027
Related Policies	Data Protection Policy Acceptable Use Policy Business Continuity Plan Risk Management Policy Information Security Policy Safeguarding Policy Critical Incident Plan
Related committee for review	Finance, Audit & Risk Committee
Approved	October 2026
Filed as	OBR Cyber Security Policy V1.0 1026

Barnet Special Education Trust

Version History

Version	Date	Author	Changes Made	Approved By
1.0	October 2026	Simon Clark	Initial policy creation	Finance, Audit & Risk Committee

1. Introduction and Purpose

This Cyber Security Policy establishes Oakbridge Special Education's approach to protecting IT systems, networks, and data from cyber threats, ensuring confidentiality, integrity and availability of data, and mitigating risks from theft, loss, misuse, damage or abuse of systems.

2. Scope

This policy applies to all staff, students, third parties, and college members who interact with college information and IT systems, including all college-owned devices and networks, cloud systems, mobile devices accessing college data and electronic communications.

3. Legal and Regulatory Framework

The college must comply with General Data Protection Regulation (GDPR) and Data Protection Act 2018, Data (Use and Access) Act 2025, Computer Misuse Act 1990, Freedom of Information Act 2000, Keeping Children Safe in Education (KCSIE) 2026. The college's safeguarding approach is set out in the Safeguarding Policy in accordance with KCSIE 2026.

3.1 Academy Trust Specific Requirements

As part of Barnet Special Education Trust, the college must comply with the Academy Trust Handbook 2025. Section 6.15 states academy trusts must not pay cyber ransom demands. Any ransom demand must be reported immediately to the CEO and authorities as outlined in Section 10.3.

4. College Obligations Under IT Service Agreement

The college acknowledges the following responsibilities as set out in the Interm IT service agreement.

Backup and Cyber Protection: The college is solely responsible for ensuring the correctness, adequacy, and security of its cloud backup and cyber protection measures. The college must purchase and maintain adequate backup solutions, implement daily backup procedures, and regularly review backup adequacy. Interm IT assists with, recommends, and configures backup solutions collaboratively, but ultimate responsibility rests with the college.

Safeguarding Monitoring: Under KCSIE 2026, the lead DSL has overarching responsibility for safeguarding which cannot be delegated. Interm IT consultants are Stage 1 safeguarding trained only and are not responsible for deciding if Senso alerts are false positives, accessing student safeguarding history, or assessing risk levels. The college retains full responsibility for Senso monitoring and safeguarding decisions.

Physical Equipment Checks: The college is responsible for termly physical checks of installed IT equipment including interactive panels, speakers, wireless access points, network cabinets, and projectors. These checks are crucial for structural safety and health and safety compliance.

MIS and Finance Software Support: The college's MIS and finance software is supported primarily by the college's MIS provider. Interm IT will assist only under direction from the MIS provider.

Administrator Access: Administrator-level access to the network requires written request from the Provision Manager for security and auditing reasons.

Cyber Insurance: The college should maintain its own cyber insurance for college-specific losses. Interm IT's cyber liability insurance (£3m per claim, £250k cyber crime) covers Interm IT's liability only.

End-of-Life Systems: Interm IT will advise the college of end-of-life hardware and out-of-support software. If the college continues to use such items following Interm IT's recommendation not to, Interm IT has no liability for any resulting loss, damage, faults, or cyber threats.

Broadband Connectivity: Interm IT cannot be held liable for loss of broadband connectivity, installation delays, faults, or connectivity speed issues.

5. Information Security Principles and Classification

The college's information security principles are:

1. Information classified by confidentiality, integrity and availability level
2. Staff with information responsibilities ensure appropriate classification and handling
3. All users handle information according to classification level
4. Information secure yet available to those with legitimate need
5. Information protected against unauthorised access and processing
6. Policy breaches must be reported
7. Information security provision regularly reviewed

The college adopts three classification levels for information:

Security Level	Definition	Examples	Protection Required
Confidential	Normally accessible only to specified members of the college. Should be held in an encrypted state outside the college systems	GDPR-defined Special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record); Passwords; Large aggregates of personally identifying data (>1000 records)	AES 256-bit encryption when stored outside college systems
Restricted	Normally accessible only to specified	GDPR-defined Personal Data (information that identifies living individuals including home/work address, age, telephone	Valid logon required;

	and/or relevant members of college staff	number, photographs); Draft reports, papers and minutes; Internal correspondence	access controls
Public	Accessible to all members of the public	Annual accounts; Minutes of statutory committees; School policy and procedures (as appropriate)	Modification restricted to authorised staff

6. Governance and Responsibilities

6.1 Responsibility Matrix

Role	Key Cyber Security Responsibilities
Governing Board	• Set policy and strategy for cyber security and risk management • Determine appropriate risk appetite • Receive termly cyber security reports covering incidents, security measures, training rates, emerging threats, and budget requirements • Review this policy annually
Provision Manager (Digital Lead: Simon Clark)	• Implement cyber security strategy • Coordinate annual cyber security risk assessments • Ensure staff training is delivered • Maintain cyber incident response plan • Present termly reports to Governing Board • Promote risk awareness across college operations
College IT Lead (Kareen Linton)	• Primary liaison with Interm IT (MSP) • Coordinate day-to-day IT operations and user support • Escalate cyber security incidents to Digital Lead • Maintain IT asset registers and documentation • Support staff IT training • Receive monthly security reports from Interm IT • Notify Interm IT within 24 hours when staff leave (for access removal)
All Staff	• Understand and identify common cyber security risks • Create and maintain strong passwords • Keep devices and data physically secure • Report phishing emails and security concerns immediately • Never share passwords or login credentials • Report lost/stolen devices immediately • Comply with acceptable use requirements

Interm IT (Managed Service Provider)	• Implement and maintain technical security controls on curriculum systems including firewalls, anti-malware, and patches. • Monitor network for automated security risks via partner systems. • Respond to and contain cyber security incidents within contracted scope and using reasonable endeavours. • Assist with, recommend, and configure backup strategies collaboratively, noting that the college retains ultimate responsibility for backup adequacy. • Configure secure access controls. • Provide monthly security status reports to college IT Lead. • Conduct security assessments on curriculum systems. • Support end-of-life systems on reasonable endeavours basis only with no liability accepted. • Provide administrator access upon written request from Provision Manager. Support MIS and finance systems under direction from college's MIS provider only.

6.2 Service Level Agreement

The college maintains an SLA with Interm IT covering cyber security response times, monitoring requirements, backup commitments, and patch management timescales. The Digital Lead and School IT Lead conduct annual performance reviews with Interm IT.

7. Cyber Security Risk Assessment

The college completes cyber security risk assessments annually and when there is a significant technology change, process change, or security incident.

Asset Management: The college maintains asset, information asset, and contracts registers covering all physical hardware, data holdings with storage details, and supplier contracts for digital services.

Assessment Activities: The college keeps the record of processing activities (ROPA) current, reviews staff access and permissions termly, verifies password policy enforcement, ensures email security measures (SPF, DKIM, DMARC) are configured, maintains network documentation with Interm IT, determines appropriate logging levels, and reviews network security configurations regularly.

Common Threats: Phishing, email impersonation, malware (including ransomware), denial of service, account takeover, unauthorised access, vishing, smishing, social engineering, whaling, insider threats, and supply chain attacks. See Appendix A for definitions.

Risk Management: Risks are recorded in the risk register, reviewed termly (minimum), and significant risks reported to the Governing Board.

8. Protection Measures

Security Area	Requirements	Responsibilities	Key Standards
8.1 CORE TECHNICAL SECURITY			
Mandatory Baseline	Boundary firewall, anti-malware on all devices, timely security patches, monthly security reports	**Interm IT:** Implement and maintain controls on curriculum systems, apply patches, provide monthly reports to college IT Lead. **Note:** Interm IT supports end-of-life systems on reasonable endeavours basis only with no liability. College must follow Interm IT recommendations on system upgrades	Firewall prevents unauthorised access, monthly status reports reviewed by college IT Lead. Interm IT not liable for broadband connectivity issues or end-of-life system failures
Access Controls	Principle of least privilege, role-based access, termly permission reviews, immediate access removal on staff departure	**College IT Lead:** Maintain user account list, coordinate termly reviews with Interm IT, notify Interm IT within 24 hours of staff departures	All users have minimum necessary access, permissions reviewed each term, access removed within 24 hours
Passwords	Minimum 3-4 random words OR machine-generated, no complexity requirements unless system-required, regular changes for privileged accounts only, never share, password managers permitted	**All Staff:** Create strong passwords, never share credentials, use password managers where appropriate	Example: "coffee-bicycle-mountain-piano", privileged accounts change regularly, standard accounts only if compromised
Multi-Factor Authentication	MFA required for all administrative accounts, email systems, cloud services, examination management systems, financial systems	**Interm IT:** Configure MFA on required systems. **All Staff:** Set up and use MFA correctly	Two or more verification methods required, protects against unauthorised access even if password compromised
8.2 DATA BACKUP			
College Backup Responsibility	College solely responsible for backup correctness, adequacy and security. Purchase and maintain adequate backup solutions with sufficient capacity. Implement daily backup procedures for on-premises and cloud-based technologies (M365 SharePoint, Google Classroom, etc.). Store backup media securely. Maintain onsite devices within warranty. Review backup procedures regularly	**College (Digital Lead & School IT Lead):** Purchase backup solutions, verify adequacy, review procedures regularly, ensure sufficient capacity. **All Staff:** Store data in shared areas not local devices	College retains ultimate responsibility for backup adequacy. Local device data is user responsibility. Data loss from local device failure is user responsibility

3-2-1 Method	At least 3 backup copies on at least 2 separate devices with at least 1 copy off-site	**Interm IT:** Assist with, recommend and configure backups collaboratively, provide backup status in monthly reports. **College IT Lead:** Coordinate termly testing with Interm IT, escalate issues to Digital Lead. **Digital Lead:** Review backup plan annually	Off-site storage protects against disasters. Interm IT uses reasonable endeavours to restore backups. If useable backup unavailable, system reconfiguration/reinstallation may incur additional college costs
Backup Testing	Termly restoration tests to verify backups work	**College IT Lead:** Coordinate termly testing with Interm IT. **Interm IT:** Conduct restoration tests using reasonable endeavours. **Digital Lead:** Review annually	If tests fail, College IT Lead escalates immediately to Digital Lead. College acknowledges potential system rebuild costs if backups fail
8.3 CLOUD SERVICES			
Provider Vetting	Complete Cloud Assurance Questionnaire before commissioning, ISO27001 certification when processing personal data	**Digital Lead & College IT Lead:** Ensure questionnaire completed, verify certifications	All cloud providers vetted before use, personal data only processed by certified providers
8.4 PHYSICAL SECURITY			
Physical Controls	Server rooms locked with restricted access, devices secured when not in use, visitors cannot access IT equipment unsupervised, mobile devices encrypted and password-protected	**Site Manager & College IT Lead:** Maintain physical security, monitor access. **All Staff:** Secure devices, challenge unauthorised visitors	Server room access restricted to authorised personnel, devices not left unattended
Physical Equipment Checks	Termly physical checks of interactive panels, speakers, wireless access points, network cabinets, and projectors for structural safety and health and safety compliance	**College Staff (coordinated by Site Manager):** Conduct termly checks report issues promptly, quarantine equipment until repairs completed. **Interm IT:** Not responsible for physical equipment checks or any loss/damage from failure to conduct checks	College responsible for maintaining safe learning environment. Interm IT not liable for failures in physical equipment maintenance
8.5 REMOTE ACCESS			
Approved Methods	VPN, secure remote desktop or approved cloud services only, no access from public/unsecured Wi-Fi without VPN, MFA required, secure private home working environment, screens not visible to others when	**College IT Lead:** Arrange remote access. **Interm IT:** Configure approved methods. **All Staff:** Use only approved methods, ensure secure environment, use privacy screens in public	Contact College IT Lead (Kareen Linton) to arrange access, VPN required for public Wi-Fi, home working area private and secure

	displaying confidential/restricted information		
8.6 PERSONAL DEVICES (BYOD)			
Permitted Use	College email and approved cloud services only, devices must have up-to-date OS with latest security patches, screen lock enabled, anti-virus installed and updated, device encryption enabled	**All Staff:** Meet security standards, report lost/stolen devices immediately to School IT Lead. **College IT Lead:** Coordinate remote wipe with Interm IT if necessary	College reserves right to remotely wipe college data from personal devices
Prohibited Use	Storing college data locally, downloading college data for offline access, using personal cloud storage for college data, accessing examination materials or candidate data, sharing college login credentials with family	**All Staff:** Comply with prohibitions	Violations may result in disciplinary action
Home Networks	Change default router passwords, enable WPA3 or WPA2 encryption, keep router firmware updated, use separate guest network where possible	**All Staff working from home:** Secure home networks, contact College IT Lead or Interm IT for support	Protects against unauthorised access, guest network isolates visitors

8.7 REMOVABLE MEDIA			
Encryption	All removable media containing college data must use AES 256-bit encryption, password-protected encrypted USB drives only, only college-issued or IT-approved removable media permitted	**College IT Lead:** Maintain register of approved media, approve and encrypt personal USB drives before use. **All Staff:** Use only approved encrypted removable media, request approval before using personal USB drives	College IT Lead coordinates with Interm IT for encryption, register maintained of all approved media
Prohibited	Connecting unknown USB drives to college systems, using removable media from untrusted sources, sharing USB drives between personal and college use without approval	**All Staff:** Comply with prohibitions.	Unknown USB drives may contain malware

Lost/Stolen	Report immediately to College IT Lead, incident logged and assessed as potential data breach	**All Staff:** Report immediately to College IT Lead (Kareen Linton). **College IT Lead:** Log incident, assess as potential data breach, coordinate with Digital Lead and DPO if necessary	Immediate reporting enables rapid response; encryption protects data even if device lost
Disposal	Never dispose in general waste, secure wipe or physical destruction required, record maintained of disposed media	**College IT Lead:** Coordinate secure disposal with Interm IT, maintain disposal records. **Interm IT:** Securely wipe or destroy media	Prevents data recovery from disposed devices, disposal records provide audit trail
8.8 EMAIL SECURITY			
Technical Measures	SPF, DKIM and DMARC configured, automatic filtering and quarantine, malicious attachment scanning, external email warnings displayed, monthly threat reports	**Interm IT:** Configure and maintain email security systems, monitor threats, provide monthly reports to College IT Lead. **College IT Lead:** Review monthly threat reports, escalate issues to Digital Lead	SPF/DKIM/DMARC prevent email spoofing and phishing, external warnings help identify potential phishing, monthly reports track blocked threats
Staff Vigilance	Be vigilant for phishing emails, never click links/open attachments from unknown senders, verify unexpected emails from known contacts, report suspicious emails immediately without forwarding, use "Report Phishing" button where available	**All Staff:** Follow email security practices, report suspicious emails to College IT Lead (Kareen Linton) or Interm IT immediately	Phishing warning signs: urgent requests, requests for passwords, unusual language from known contacts, unexpected attachments, suspicious sender addresses

Sending Sensitive Data	Encrypt emails containing confidential data, check recipient addresses carefully, use BCC for multiple external recipients, contact College IT Lead for encryption assistance	**All Staff:** Encrypt confidential data, verify recipients, use BCC appropriately. **College IT Lead:** Assist with encryption	Confidential data = classification level "Confidential" (Section 5), BCC protects email addresses, encryption prevents interception
Prohibited	Forwarding college emails to personal accounts, using personal email for college business, sharing login credentials via email, responding to password reset requests via email, auto-forwarding to external addresses	**All Staff:** Comply with prohibitions	Personal email lacks college security controls, legitimate IT support never requests passwords via email
Retention	Retention periods per college's data retention policy, safeguarding /complaint emails retained per specific schedules	**All Staff:** Do not delete emails required for legal, regulatory or business purposes. **Interm IT:** Maintain email backups	Different email types have different retention requirements, backups enable recovery
8.9 MOBILE DEVICES			
College-Owned Mandatory Settings	Enrolled in Interm IT's MDM system, remote wipe capability enabled, full device encryption, automatic screen lock (maximum 5 minutes), up-to-date OS and security patches, "Find My Device" tracking enabled, strong password/PIN (minimum 6 digits) or biometric, Bluetooth disabled when not in use, block automatic connection to unknown Wi-Fi	**Interm IT:** Configure MDM system, enforce security settings, manage remote wipe. **College IT Lead:** Coordinate device setup, liaise with Interm IT. **All Staff:** Maintain device security settings, do not disable security features	MDM allows central management, remote wipe protects data if lost/stolen, encryption protects data if compromised, screen lock prevents unauthorised access
Lost/Stolen College Devices	1. Report immediately to College IT Lead (Kareen Linton), 2. Report to police if stolen (obtain crime reference), 3. Complete incident report, 4. College will locate and	**Staff:** Follow immediate actions. **College IT Lead:** Coordinate with Interm IT for location/remote	Immediate reporting enables rapid response, remote wipe prevents data access, police

	remotely wipe if necessary, 5. Assess data breach	wipe, notify Digital Lead, complete incident assessment. **Interm IT:** Attempt location, execute remote wipe if required	report required for insurance
Personal Devices On Premises	Not used to photograph/record students without explicit permission (ChatPro app only), not connected to main network (guest Wi-Fi only), not used to access/store confidential college data, kept secure not left unattended, Personal mobile phones must remain secured in authorised lockable pouches during the college day unless use is required for an approved business purpose or authorised by Provision Manager	**All Staff:** Comply with restrictions. **Provision Manager:** Authorise exceptions where appropriate	Protects students privacy and safeguarding, guest Wi-Fi isolates personal devices from college network
Devices Off-Site	Kept secure always, not left in vehicles overnight, not left unattended in public, transported in non-descript bags, privacy screens used in public spaces, returned to college and secured when not in use	**All Staff:** Follow off-site security requirements	Non-descript bags reduce theft risk, privacy screens prevent shoulder surfing, vehicles not secure overnight storage
8.10 FILTERING AND MONITORING			
LGfL Filtering	Blocks illegal content (child sexual abuse imagery, terrorist content), blocks harmful material inappropriate for student age/maturity, age-appropriate proportionate filtering policies, regular updates for emerging threats, allows appropriate educational internet use, provides reporting and analytics	**Interm IT:** Manage LGfL filtering system, apply updates, provide reporting. **College IT Lead:** Liaise with Interm IT on functionality, conduct termly effectiveness spot checks, report technical issues immediately, process unblocking requests	Complies with KCSIE 2026, protects students from harmful content, balances protection with educational freedom
Senso Monitoring	Records internet usage and flags concerning activity in real-time, **sends automated email alerts directly to DSL and Digital Lead** for potentially harmful content,	**Senso System:** Automatically emails alerts to DSL (Kareen Linton, Lorraine O'Brien) and Digital Lead (Simon Clark). **College IT Lead (Kareen Linton):**	Alerts categorised by severity (low, medium, high, critical) with **automated**

	monitors keywords/phrases indicating safeguarding concerns, captures screenshots of concerning activity, identifies patterns indicating safeguarding concerns, operates per data protection requirements, monitors college-owned devices on and off network. **Important: Senso licensed to Interm IT and will be removed if contract terminates**	Review alerts daily during term **in addition to automated emails**, log alerts and actions, provide monthly activity reports to Digital Lead, ensure appropriate configuration, test alert system termly. **DSL (Kareen Linton, Lorraine O'Brien):** Receive automated email alerts and respond to monitoring-identified concerns, determine appropriate responses including external referrals, provide feedback on effectiveness, participate in annual review. **Note: Interm IT consultants are Stage 1 safeguarding trained only and are NOT responsible for deciding if alerts are false positives, accessing child safeguarding history, or assessing risk levels. Under KCSIE 2026, lead DSL has overarching safeguarding responsibility which cannot be delegated**	**email notification to DSL and Digital Lead** for immediate escalation of safeguarding concerns. Monitoring helps identify when students need support. Keywords and thresholds reviewed termly. College IT Lead and DSL retain full responsibility for all Senso monitoring and safeguarding decisions
Staff Responsibilities	Understand filtering/monitoring protects students, report student online activity concerns to DSL (Kareen Linton, Lorraine O'Brien), never attempt to bypass filtering systems, report filtering failures to College IT Lead immediately, aware their internet usage is also monitored	**All Staff:** Comply with filtering/monitoring requirements, report concerns and failures	Staff monitoring ensures acceptable use compliance, bypassing filtering is a disciplinary matter
Annual Review (Summer Term)	Review assesses effectiveness of LGfL filtering and Senso monitoring, gaps/weaknesses identified during year, incidents where harmful content accessed despite filtering, safeguarding concerns identified and handled, alert thresholds and	**Review Team:** Digital Lead (Simon Clark), DSL (Kareen Linton, Lorraine O'Brien), College IT Lead (Kareen Linton), Interm IT (technical support). **Digital Lead:** Present review to Governing Board, use for budget planning, share with	Review documented using standard template, includes analysis of monitoring data from past year, includes action plan for

	keyword appropriateness, false positive rates, emerging threats relevant to pupil population, compliance with statutory guidance, whether systems remain fit for purpose	Interm IT for technical changes, retain as compliance evidence	improvements, required by KCSIE 2026
Communication	Students informed about filtering/monitoring in online safety education, students aware monitoring keeps them safe not invading privacy, students aware monitoring applies on and off premises, information in parent communications especially for home device use, transparent approach in prospectus and website, guidance to parents on home online safety	**Digital Lead & DSL:** Ensure appropriate communications, provide online safety education, engage parents	Transparency builds trust, students understand monitoring purpose, parents supported to reinforce online safety at home
Data Protection	Senso data processed per UK GDPR and Data Protection Act 2018, only authorised staff (College IT Lead and DSL) access monitoring data, data retained only as long as necessary for safeguarding, pupils and parents informed via privacy notices, monitoring proportionate and necessary, regular proportionality reviews	**College IT Lead & DSL:** Limit access to monitoring data, ensure appropriate retention. **Digital Lead:** Conduct proportionality reviews	Balances safeguarding duty with privacy rights, privacy notices ensure transparency, proportionality reviews ensure monitoring remains appropriate

9. Staff Training and Awareness

Annual staff training covers identifying cyber security risks, reducing breach risk, creating strong passwords, securing devices and data, dealing with phishing attacks, and responding to data breaches.

Governor training ensures governors understand cyber attack threats.

Student education follows Education for a Connected World guidance, providing age-appropriate cyber security learning, adapted to suit the needs of our learners.

10. Incident Response

10.1 Reporting Incidents

All staff must report any suspected cyber security incident immediately, including suspicious emails, lost or stolen devices, malware infections, unusual system behaviour, unauthorised access, accidental data disclosure, ransomware, or other security concerns.

What to Report and How: See Appendix B for detailed guidance on what to report and information required. It is always better to report a concern that proves harmless than to fail to report a serious issue.

Primary contacts:

Incident Type	Contact	Details
IT technical support & immediate response	College IT Lead: Kareen Linton	kareen.linton@bsentrust.org Oakbridge Student Reception office
MSP technical support	Interm IT Helpdesk	sd@intermit.co.uk 01763 272 765 www.IntermIT.co.uk
Strategic decisions & escalation	Digital Lead: Simon Clark (Provision Manager)	simon.clark@oakbridgesen.org 07539329597
Provision Manager absence	Deputy Provision Manager: Lorraine O'Brien	lorraine.o'brien@oakbridgesen.org 02030260611
Phishing emails	College IT Lead or Interm IT	Use "Report Phishing" button if available
Data breaches	Colleg IT Lead, Digital Lead, DSL & DPO	DSL: Kareen Linton (kareen.linton@bsentrust.org), Lorraine O'Brien (lorraine.o'brien@oakbridgesen.org) DPO: Satswana (info@satswana.com / 01252 759177) RPA Insurers: Contact if breach may result in insurance claim Police: Contact if breach involves criminal activity or stolen devices Cyber Alarm: Contact for cyber security incident support RPA Insurers Police Cyber Alarm

Lost/stolen devices	College IT Lead	Coordinates remote wipe with Interm IT Also notify Digital Lead
System outages/cyber attacks	Interm IT Helpdesk, then College IT Lead	College IT Lead escalates to Digital Lead
Out of hours emergency	Interm IT Emergency Line, then email Digital Lead	Follow up with College IT Lead next working day
Trust-level escalation	CEO: Lynda Walker	lynda.walker@bsentrust.org 07944 602021

10.2 Immediate Response

If experiencing a cyber attack, staff should remain calm, disconnect affected devices from the network where safe, photograph on-screen messages, note the time, preserve evidence, and immediately contact the College IT Lead Kareen Linton, Interm IT Helpdesk at sd@intermit.co.uk or 01763 272 765, and Digital Lead Simon Clark at 07539329597.

Staff must not turn off devices, pay ransom demands (Academy Trust Handbook prohibition in Section 3.1), attempt self-recovery, delete evidence, discuss on social media, or share information with unverified individuals.

See Appendix B for detailed immediate response procedures.

10.3 External Reporting

The college must report security breaches to Action Fraud at 0300 123 2040 or www.actionfraud.police.uk and the DfE sector cyber team at sector.incidentreporting@education.gov.uk.

The college may also need to report to the National Cyber Security Centre (NCSC) if the incident causes long-term college closure, closure of multiple schools/colleges, or serious financial damage, to the Information Commissioner's Office (ICO) within 72 hours for high-risk data breaches via the DPO, to the college's cyber insurance provider if applicable.

Note on Broadband and Connectivity Issues: If a cyber incident involves or is caused by broadband connectivity issues, the college should note that Interm IT cannot be held liable for loss of broadband connectivity, installation delays, faults, or connectivity speed under the service agreement. The college should contact its broadband provider (LGFL) directly for connectivity issues.

10.5 Data Breach Response

Suspected breaches of personal data must be reported to the college's Data Protection Officer service. The DPO will investigate any reported breach to determine whether a material breach has occurred and report to the Information Commissioner's Office within 72hrs of receiving an alert.

11. Business Continuity and Disaster Recovery

The college maintains a cyber response plan to limit disruption to teaching and learning if a cyber attack prevents access to IT systems or data.

Plan Contents: The plan defines what constitutes a digital technology disaster, details the disaster recovery team and key contacts, outlines testing procedures for the recovery plan, describes the digital technology risk assessment process, identifies risk reduction steps, and specifies recovery actions if risk occurs.

Plan Management: Plans are maintained in printed form for emergency access and stored online in a secure cloud location accessible to the disaster recovery team. Plans are reviewed annually or when significant digital technology changes occur.

Backup Restoration Limitations: The business continuity plan must acknowledge that if backup restoration is required, Interm IT will use reasonable endeavours but if a useable backup is not available, fresh system reconfiguration or reinstallation may be necessary at additional cost to the college. The plan should include budget contingency for potential system rebuild costs and identify alternative data sources where possible.

12. Acceptable Use

The college will maintain an acceptable use policy to set out expectations for how staff and students should use the college's digital technology, including acceptable use agreements to sign.

Key requirements include:

- No personal use of college devices for storing sensitive data
- No installation of unauthorised software
- No sharing of passwords or login credentials
- Immediate reporting of lost or stolen devices
- Compliance with email and internet usage policies

13. Supplier and Third-Party Management

All college suppliers will abide by the college's Information Security Policy or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- When accessing or processing college assets, whether on site or remotely
- When subcontracting to other suppliers

13.1 Managed Service Provider

The college's primary IT supplier is Interm IT, providing 16 hours weekly on-site support during term time (39-40 weeks annually) plus 16-hour pre-autumn term visit. The college maintains an SLA covering incident response times, security monitoring, backup assistance, and patch management. The College IT Lead (Kareen Linton) manages day-to-day liaison and escalates concerns to the Digital Lead.

Service Scope: Interm IT provides curriculum hardware and software support. For MIS and finance systems, contact the college's MIS provider first; Interm IT assists only under MIS provider direction. Interm IT manages the network with full administration rights and may install software (Senso, K9 Dock, K9 User Manager) licensed to Interm IT and removed upon contract termination. Administrator access requires written Provision Manager request.

Service Exclusions: Interm IT is not liable for broadband connectivity issues, supports end-of-life systems on reasonable endeavours basis only with no liability, assists with backups collaboratively but college retains sole responsibility for backup adequacy, has consultants Stage 1 safeguarding trained only with college retaining full Senso monitoring and safeguarding responsibility, is not responsible for termly physical equipment checks, and may charge additional costs for third-party hardware configuration. If backups fail, system reconfiguration or reinstallation may incur additional college costs.

Oversight: Annual reviews of certifications, insurance (£3m cyber liability covering Interm IT's liability only), and performance. College should maintain separate cyber insurance for college-specific losses.

13.2 Other Suppliers

For all other suppliers with access to college systems or data, the college will:

- Maintain a register of all third-party suppliers with system access (maintained by College IT Lead)
- Ensure data processing agreements are in place before granting access
- Review supplier security annually (coordinated by Digital Lead)
- Require ISO27001 certification for cloud services processing personal data
- Conduct due diligence before appointing new suppliers
- Ensure suppliers notify the college immediately of any security incidents affecting college data

The college IT Lead will maintain the supplier register and coordinate with Interm IT to ensure appropriate access controls are in place for all third-party suppliers.

14. Monitoring and Review

This policy will be reviewed annually to sustain its effectiveness.

The review will include:

- Assessment of cyber security incidents during the year
- Evaluation of the effectiveness of controls
- Updates to reflect changes in technology or threats
- Feedback from staff, governors, and external audits
- Results of penetration testing (where conducted)

The Digital Lead will present an annual cyber security report to the Governing Board covering:

- Summary of incidents and responses
- Status of risk mitigation measures
- Training completion rates

- Recommendations for improvement
- Budget requirements for cyber security

14.1 Testing and Audit Schedule

To ensure the effectiveness of cyber security measures, the college will conduct regular testing and audits:

Activity	Frequency	Responsible	Reported To
Full backup restoration test	Annually	Interm IT (coordinated by College IT Lead)	Digital Lead
Backup verification	Termly	Interm IT	College IT Lead
Disaster recovery plan test	Annually	Digital Lead, College IT Lead & Interm IT	Governing Board
Penetration testing (if budget allows)	Every 2 years	External provider (arranged via Interm IT)	Governing Board
Access rights review	Termly	College IT Lead & Interm IT	Digital Lead
Password policy compliance check	Termly	Interm IT	College IT Lead
Phishing simulation exercise	Twice yearly	Interm IT	Digital Lead via College IT Lead
Physical security audit	Annually	Site Manager, College IT Lead & Digital Lead	Governing Board
Supplier security review	Annually	Digital Lead & College IT Lead	Finance, Audit & Risk Committee
MSP (Interm IT) performance review	Annually	Digital Lead & College IT Lead	Governing Board
Policy review and update	Annually	Digital Lead	Governing Board
Filtering and monitoring system review	Annually (summer term)	Digital Lead, DSL, College IT Lead & Interm IT	Governing Board

Filtering effectiveness test	Termly	College IT Lead & Interm IT	Digital Lead
Monitoring alert system test	Termly	College IT Lead & Interm IT	DSL (Kareen Linton, Lorraine O'Brien)

14.2 Test Documentation

All tests and audits must be documented, including:

- Date and time of test
- Personnel involved (including Interm IT staff where applicable)
- Test procedures followed
- Results and findings
- Any issues identified
- Remedial actions required
- Sign-off by responsible person

The College IT Lead will maintain a central log of all testing activities and outcomes, reporting significant findings to the Digital Lead.

14.3 Failed Tests

If any test fails or identifies significant issues, the College IT Lead must escalate immediately to the Digital Lead (Provision Manager), a remedial action plan must be created within 5 working days coordinated by the College IT Lead with Interm IT, the Governing Board must be informed at the next meeting, and the test must be repeated once remedial actions are complete.

14.4 Cyber Essentials Certification

The college recognises that Cyber Essentials certification is recommended by the Department for Education and the National Cyber Security Centre as a baseline standard for cyber security.

Commitment to Cyber Essentials

The college recognises Cyber Essentials certification as the Department for Education and National Cyber Security Centre recommended baseline standard.

Commitment: Subject to budget availability, the college will work towards Cyber Essentials certification, use the framework as a benchmark for controls, review progress annually, and include certification costs in budget planning.

Five Key Controls: The Cyber Essentials scheme covers firewalls protecting internet connections, secure configuration ensuring systems are configured securely, access control controlling data and service access, malware protection protecting against malicious software, and patch management keeping systems updated. See Section 8.1 for implementation details.

The College IT Lead works with Interm IT to ensure controls are implemented and maintained in line with Cyber Essentials requirements.

15. Policy Compliance

Security breaches could result in loss of confidentiality, integrity, and availability of personal or confidential data. Personal data breaches infringe GDPR and may result in criminal or civil action against the school.

Non-Compliance Consequences: Non-compliance with this policy may result in disciplinary action in accordance with college policies, removal of system access privileges, referral to external authorities where appropriate.

All staff must confirm annually they have read and understood this policy.

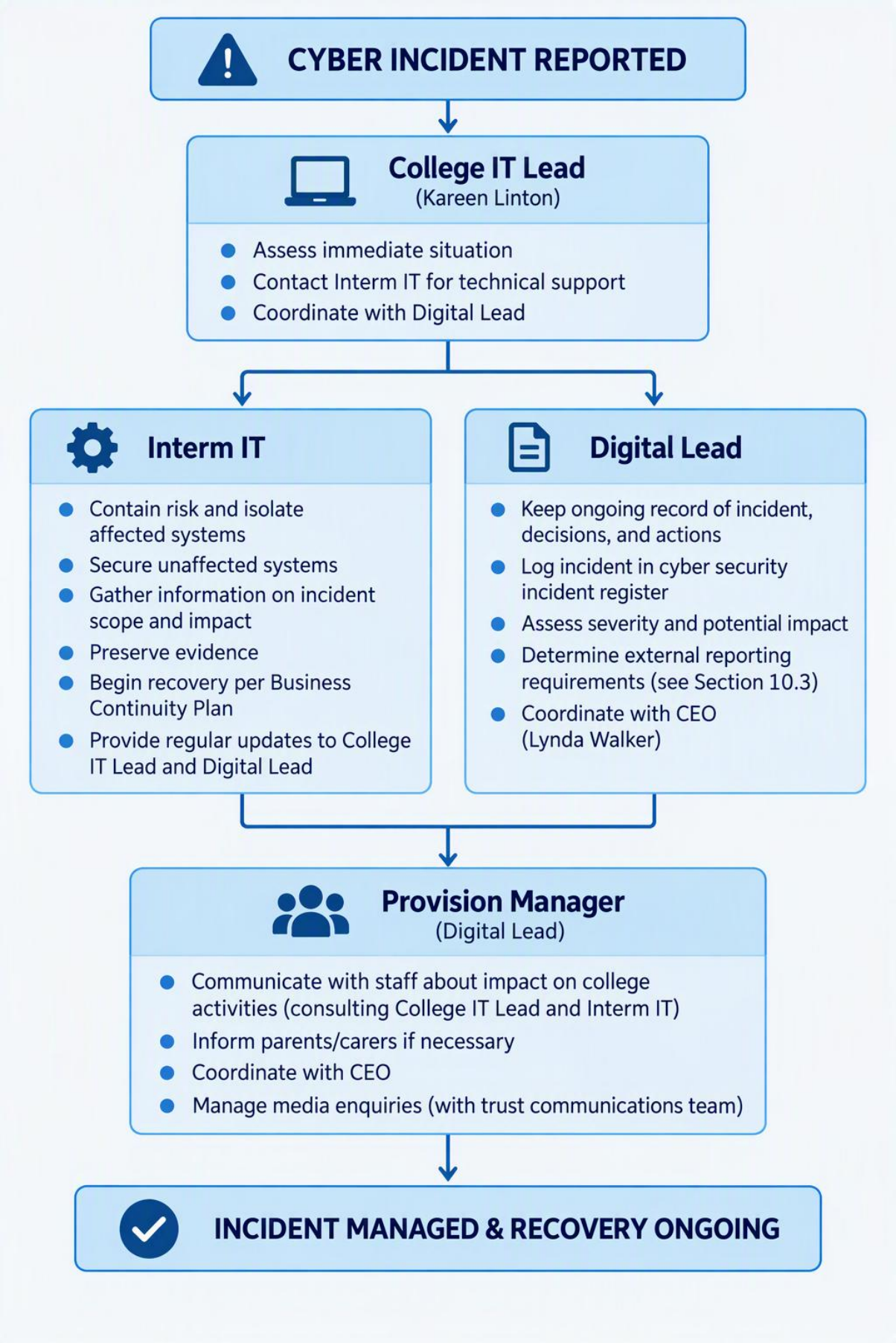
Appendix A: Glossary of Cyber Security Terms

Term	Definition
AES 256-bit encryption	Advanced Encryption Standard using a 256-bit key - a very strong form of encryption used to protect sensitive data
Anti-malware	Software designed to detect, prevent, and remove malicious software (malware)
Backup	A copy of data stored separately so it can be restored if the original is lost or damaged
BYOD (Bring Your Own Device)	A policy allowing staff to use personal devices for work purposes
Cloud services	Computing services (storage, software, etc.) delivered over the internet rather than from local servers
Cyber attack	An attempt to damage, disrupt, or gain unauthorised access to computer systems or networks
Data breach	An incident where confidential, sensitive, or protected data is accessed, disclosed, or stolen without authorisation
DMARC	Domain-based Message Authentication, Reporting & Conformance - an email security protocol
Encryption	The process of converting data into a code to prevent unauthorised access
Firewall	A security system that monitors and controls incoming and outgoing network traffic
GDPR	General Data Protection Regulation - EU/UK law governing data protection and privacy
ISO27001	International standard for information security management systems
Malware	Malicious software designed to damage or gain unauthorised access to systems (includes viruses, ransomware, spyware)
MDM (Mobile Device Management)	Software that allows remote management and security of mobile devices
MFA (Multi-Factor Authentication)	Security process requiring two or more verification methods to access a system

MSP (Managed Service Provider)	External company providing IT services and support (Interm IT for Oakbridge Special Education)
Patch	A software update that fixes security vulnerabilities or bugs
Penetration testing	Simulated cyber attack to test the security of systems
Phishing	Fraudulent emails or messages attempting to trick people into revealing sensitive information
Ransomware	Malware that encrypts data and demands payment for its release
Remote wipe	The ability to delete data from a device remotely, typically used if a device is lost or stolen
Smishing	Phishing via SMS text messages
Social engineering	Manipulation techniques used to trick people into revealing confidential information
Spyware	Malware that secretly monitors and collects information about users
USB drive	Portable storage device that connects via USB port (also called flash drive or memory stick)
Vishing	Phishing via voice calls (voice phishing)
VPN (Virtual Private Network)	Secure connection that encrypts data when accessing networks remotely
Whaling	Highly targeted phishing attack aimed at senior staff members

Appendix B: Cyber Security Incident Reporting .




CYBER INCIDENT REPORTED
College IT Lead
(Kareen Linton)
Assess immediate situation
Contact Interm IT for technical support
Coordinate with Digital Lead
Interm IT
Contain risk and isolate affected systems
Secure unaffected systems
Gather information on incident scope and impact
Preserve evidence
Begin recovery per Business Continuity Plan
Provide regular updates to College IT Lead and Digital Lead
Digital Lead
Keep ongoing record of incident, decisions, and actions
Log incident in cyber security incident register
Assess severity and potential impact
Determine external reporting requirements (see Section 10.3)
Coordinate with CEO (Lynda Walker)
Provision Manager
(Digital Lead)
Communicate with staff about impact on college activities (consulting College IT Lead and Interm IT)
Inform parents/carers if necessary
Coordinate with CEO
Manage media enquiries (with trust communications team)
INCIDENT MANAGED & RECOVERY ONGOING

If experiencing a possible cyber attack right now:

STOP
THINK
FOLLOW
PROTECT

OUR COLLEGE
OUR DATA
OUR FUTURE

DO:

TAKE THESE STEPS TO HELP KEEP PEOPLE, DATA AND SYSTEMS SAFE

1. Stay calm and follow these procedures.
2. Disconnect from network (unplug cable or disable Wi-Fi) if safe to do so.
3. Photograph on-screen messages with your mobile phone.
4. Note the time of discovery.
5. Preserve physical evidence (USB drives, emails, materials).
6. Contact immediately:

College IT Lead: Kareen Linton

Interm IT Helpdesk: sd@intermit.co.uk / 01763 272 765

Digital Lead: Simon Clark – 07539329597

Out of hours: Interm IT Emergency Line

DO NOT:

AVOID THESE ACTIONS – THEY MAY MAKE THE SITUATION WORSE

1. Panic.
2. Turn off affected devices (may destroy evidence).
3. Pay any ransom demands (see Section 3.1 - Academy Trust Handbook prohibition).
4. Attempt recovery yourself unless you are College IT Lead or Interm IT.
5. Delete files or evidence.
6. Discuss on social media.
7. Provide information to anyone claiming to be technical support without verifying identity.

REPORT | PRESERVE | PROTECT

WORKING TOGETHER FOR A SAFER COLLEGE

PEOPLE SAFE
DATA SECURE
LEARNING CONTINUES