

Cyber Security Policy



Burnham on Crouch Primary School

Connected to our world

Staff consulted: Aut26

Ratified by the Governing Body: Aut26

Review date: Aut27

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Access management
5. Passwords and authentication
6. Device and endpoint security
7. Network security, filtering and monitoring
8. Email, phishing and malicious content
9. Data protection and secure information handling
10. Backup, disaster recovery and business continuity
11. Remote working and personal devices
12. Staff training and awareness
13. Reporting and responding to cyber incidents
14. Monitoring arrangements
15. Links with other policies

Appendix 1 – Staff Cyber Security Checklist

Appendix 2 – Annual Governor Cyber Assurance Checklist

Appendix 3 – Cyber Incident Log

Appendix 4 – Key Contacts

1. Aims

At Burnham-on-Crouch Primary School, we recognise that effective cyber security is fundamental to safeguarding children, protecting personal and sensitive information, maintaining operational continuity, and ensuring confidence in the school's digital infrastructure.

This policy aims to:

- Protect pupils, staff, governors, volunteers and visitors from cyber threats
- Protect school systems, devices, networks and cloud-based services from loss, compromise or attack
- Ensure compliance with current Department for Education (DfE), National Cyber Security Centre (NCSC), UK GDPR and Data Protection requirements
- Support the school's safeguarding responsibilities, recognising that cyber security, online safety and safeguarding are interrelated
- Establish clear procedures for preventing, identifying, reporting and responding to cyber incidents
- Promote a culture of cyber awareness across the whole school community

2. Legislation and Guidance

This policy is based on:

- Keeping Children Safe in Education
- DfE Cyber Security Standards for Schools and Colleges
- DfE Meeting Digital and Technology Standards in Schools
- National Cyber Security Centre guidance
- UK GDPR
- Data Protection Act 2018

This policy should be read alongside the school's Online Safety Policy, Child Protection and Safeguarding Policy, Data Protection Policy, Staff Code of Conduct and Acceptable Use Agreements.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for cyber security and for holding the Headteacher to account for implementation.

The governing board will:

- Monitor implementation of this policy
- Receive annual cyber security updates
- Ensure appropriate investment in secure systems and infrastructure
- Review cyber risks as part of safeguarding and business continuity planning
- Ensure filtering and monitoring arrangements remain effective

The governor with oversight of online safety and cyber security is:

Chair of Governors - Joel Tunbridge

3.2 The Headteacher

The Headteacher is responsible for:

- Ensuring this policy is implemented consistently across the school
- Ensuring cyber security remains an embedded safeguarding priority
- Ensuring staff training is completed
- Supporting incident response and recovery
- Reporting significant incidents to governors where appropriate

3.3 The Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Ensuring cyber security remains an interrelated safeguarding priority
- Understanding the filtering and monitoring systems used across school devices and networks
- Ensuring cyber safeguarding concerns are logged appropriately
- Working with IT support during incidents
- Ensuring cyber incidents involving children are managed in line with safeguarding procedures

3.4 IT Support Provider

Burnham-on-Crouch Primary School works in partnership with **DL Solutions**.

Named technician:

Lee Precious

DL Solutions are responsible for:

- Firewall management
- Antivirus and endpoint protection
- Patch management
- Server maintenance
- Vulnerability checks
- Backup monitoring
- Recovery support
- Filtering and monitoring
- Incident response support

DL Solutions work closely with the Headteacher and DSL to ensure systems remain secure and compliant.

3.5 All Staff

All staff are responsible for:

- Understanding this policy
- Maintaining cyber awareness
- Following acceptable use procedures

- Reporting suspicious activity immediately
- Protecting devices and credentials
- Attending annual training and updates

4. Access Management

Burnham-on-Crouch Primary School operates robust role-based access controls.

The school ensures:

- Every staff member has an individual login
- Shared accounts are avoided wherever possible
- Permissions are reviewed regularly
- Accounts are disabled promptly when staff leave employment
- Administrative access is restricted to authorised personnel only

Multi-Factor Authentication

To strengthen account security, Burnham-on-Crouch Primary School has implemented multi-factor authentication (MFA) across key safeguarding and communication systems.

This currently includes:

- Microsoft 365 school email
- CPOMS

The Headteacher, DSL and DL Solutions review access permissions and authentication arrangements regularly.

5. Passwords and Authentication

All staff must:

- Use strong passwords (minimum 12 characters where systems allow)
- Use unique passwords across systems
- Never share passwords
- Never write passwords where they may be visible
- Change passwords immediately if compromise is suspected

In addition:

- Staff must never approve an unexpected MFA request
- Unexpected authentication prompts must be reported immediately
- Authentication devices must be kept secure and not shared

Any concerns must be reported immediately to:

- Headteacher
- DSL
- DL Solutions

6. Device and Endpoint Security

All school devices must:

- Be password protected
- Lock automatically when inactive
- Run supported operating systems
- Receive security updates promptly
- Have approved antivirus protection installed
- Have encrypted storage where possible

Staff must not:

- Install unauthorised software
- Disable security settings
- Allow family members or friends to use school devices

Lost or stolen devices must be reported immediately.

7. Network Security, Filtering and Monitoring

Burnham-on-Crouch Primary School maintains filtering and monitoring systems in line with Department for Education requirements.

The Headteacher, DSL and DL Solutions jointly oversee:

- Firewall protection
- Content filtering
- Monitoring alerts
- Network security reviews
- Vulnerability checks

The school's systems are designed to block:

- Harmful content
- Extremist content
- Malware
- Phishing websites

- Inappropriate downloads

Filtering arrangements are reviewed at least annually.

Any concerns regarding filtering or monitoring failures must be reported immediately.

8. Email, Phishing and Malicious Content

All staff must:

- Carefully check unexpected emails
- Verify unusual requests verbally where appropriate
- Never share passwords via email
- Never click suspicious links
- Never open suspicious attachments
- Report suspicious emails immediately

Suspected phishing attempts must be reported immediately.

9. Data Protection and Secure Information Handling

Sensitive information must:

- Only be stored on approved systems
- Never be transferred using personal email accounts
- Only be accessed by authorised users
- Be encrypted where appropriate

This includes systems such as:

- CPOMS
- Microsoft 365
- Evidence Me
- Showbie
- Other approved school platforms

Any suspected data breach must be reported immediately.

10. Backup, Disaster Recovery and Business Continuity

DL Solutions maintain secure backup arrangements for critical school infrastructure.

Backup arrangements include:

- Automated daily backups
- Secure cloud or off-site storage
- Routine recovery testing
- Disaster recovery support

Critical systems include:

- Safeguarding records
- Curriculum files
- Assessment information
- Staffing documentation
- Financial documentation

11. Remote Working and Personal Devices

When working remotely, staff must:

- Use school-approved devices where possible
- Access school systems only through approved secure platforms
- Avoid unsecured public Wi-Fi
- Keep devices physically secure
- Ensure screens are not visible to unauthorised individuals

Personal devices used for school business must:

- Be password protected
- Be updated regularly
- Not store sensitive data locally
- Only access approved systems

12. Staff Training and Awareness

All staff will receive:

- Cyber security induction
- Annual safeguarding training
- Phishing awareness updates
- Emerging cyber threat updates

- System-specific security updates where required

Cyber security forms part of staff induction, annual safeguarding training and ongoing safeguarding updates.

In line with Burnham-on-Crouch Primary School's proactive safeguarding culture, emerging cyber risks, phishing trends, data protection updates and digital safeguarding concerns are shared regularly through:

- Staff briefings
- Safeguarding communications
- Training updates
- Professional dialogue
- Emerging risk alerts throughout the academic year

Governors will receive annual cyber security updates as part of safeguarding training.

13. Reporting and Responding to Cyber Incidents

Examples of reportable incidents include:

- Phishing attempts
- Malware alerts
- Ransomware
- Lost devices
- Unauthorised access
- Suspicious downloads
- Compromised accounts
- Data breaches
- Filtering failures

All incidents must be reported immediately to:

1. Headteacher
2. DSL
3. DL Solutions

Where required, incidents may be escalated to:

- Information Commissioner's Office (ICO)
- National Cyber Security Centre (NCSC)
- Police
- Local Authority Data Protection Officer

Incident Response Process

Identify

Assess the nature and severity of the incident.

Contain

Isolate affected devices or systems where safe to do so.

Investigate

The Headteacher, DSL and DL Solutions determine scope, impact and safeguarding implications.

Recover

Systems are safely restored.

Review

Lessons learned are incorporated into future practice, training and risk assessments.

14. Monitoring Arrangements

This policy will be reviewed annually by:

- Headteacher
- DSL
- Computing Lead
- DL Solutions
- Governing Board

An annual cyber security risk assessment will support this review.

This policy will also be reviewed following:

- Significant cyber incidents
- Major changes to DfE guidance
- Changes to school systems or infrastructure

15. Links with Other Policies

This policy should be read alongside:

- Online Safety Policy
- Child Protection and Safeguarding Policy
- Data Protection Policy
- Staff Code of Conduct
- Behaviour Policy
- Acceptable Use Agreements
- Business Continuity Plan

Appendix 1 – Staff Cyber Security Checklist

Question	Yes / No
Do I use strong passwords?	
Is MFA enabled on my accounts?	
Do I recognise phishing emails?	
Do I lock devices when unattended?	
Do I report suspicious activity immediately?	
Do I store sensitive information securely?	
Have I completed annual cyber security training?	

Appendix 2 – Annual Governor Cyber Assurance Checklist

Question	Yes / No
Has the policy been reviewed?	
Has staff training been completed?	
Have filtering and monitoring arrangements been reviewed?	
Have backup systems been tested?	
Is MFA operational across key systems?	
Have cyber incidents been reviewed?	

Appendix 3 – Cyber Incident Log

Date System affected Nature of incident Action taken Logged by



Burnham on Crouch
Primary School
Connected to our world

APPENDIX 3 – CYBER SECURITY INCIDENT REPORT FORM

This form must be used to report and record any cyber security incident.

Please complete all relevant sections as fully as possible.

1. INCIDENT DETAILS Date of incident: _____ Time of incident: _____ Date reported: _____ Time reported: _____ Reported by: _____ Role: _____	2. NATURE OF INCIDENT (tick all that apply) <table><tr><td>☐ Suspicious email / phishing attempt</td><td>☐ Data breach / potential data breach</td></tr><tr><td>☐ Unexpected MFA authentication request</td><td>☐ Filtering or monitoring concern</td></tr><tr><td>☐ Malware / virus alert</td><td>☐ Suspicious website or download</td></tr><tr><td>☐ Lost or stolen device</td><td>☐ Ransomware or system lockout</td></tr><tr><td>☐ Unauthorised access attempt</td><td>☐ Accidental sharing of sensitive information</td></tr><tr><td>☐ Account compromise</td><td>☐ Other: _____</td></tr></table>	☐ Suspicious email / phishing attempt	☐ Data breach / potential data breach	☐ Unexpected MFA authentication request	☐ Filtering or monitoring concern	☐ Malware / virus alert	☐ Suspicious website or download	☐ Lost or stolen device	☐ Ransomware or system lockout	☐ Unauthorised access attempt	☐ Accidental sharing of sensitive information	☐ Account compromise	☐ Other: _____									
☐ Suspicious email / phishing attempt	☐ Data breach / potential data breach																					
☐ Unexpected MFA authentication request	☐ Filtering or monitoring concern																					
☐ Malware / virus alert	☐ Suspicious website or download																					
☐ Lost or stolen device	☐ Ransomware or system lockout																					
☐ Unauthorised access attempt	☐ Accidental sharing of sensitive information																					
☐ Account compromise	☐ Other: _____																					
3. SYSTEM / DEVICE AFFECTED (tick all that apply) <table><tr><td>☐ Microsoft 365 email</td><td>☐ Wi-Fi / network</td></tr><tr><td>☐ CPOMS</td><td>☐ Evidence Me</td></tr><tr><td>☐ Staff laptop</td><td>☐ Showbie</td></tr><tr><td>☐ Classroom device</td><td>☐ Other: _____</td></tr><tr><td>☐ Server / shared drive</td><td></td></tr></table> Asset / device name (if known): _____	☐ Microsoft 365 email	☐ Wi-Fi / network	☐ CPOMS	☐ Evidence Me	☐ Staff laptop	☐ Showbie	☐ Classroom device	☐ Other: _____	☐ Server / shared drive		4. DESCRIPTION OF INCIDENT (Please include what happened, how it was identified, and any relevant screenshots, messages, emails or alerts.) _____ _____ _____ _____ _____											
☐ Microsoft 365 email	☐ Wi-Fi / network																					
☐ CPOMS	☐ Evidence Me																					
☐ Staff laptop	☐ Showbie																					
☐ Classroom device	☐ Other: _____																					
☐ Server / shared drive																						
5. IMMEDIATE ACTIONS TAKEN (tick all that apply) <table><tr><td>☐ Device disconnected from network</td></tr><tr><td>☐ Password reset</td></tr><tr><td>☐ MFA reset</td></tr><tr><td>☐ Device powered down</td></tr><tr><td>☐ Email quarantined / deleted</td></tr><tr><td>☐ User account disabled</td></tr><tr><td>☐ DL Solutions informed</td></tr><tr><td>☐ Headteacher informed</td></tr><tr><td>☐ DSL informed</td></tr><tr><td>☐ Safeguarding concern identified</td></tr><tr><td>☐ Other: _____</td></tr></table>	☐ Device disconnected from network	☐ Password reset	☐ MFA reset	☐ Device powered down	☐ Email quarantined / deleted	☐ User account disabled	☐ DL Solutions informed	☐ Headteacher informed	☐ DSL informed	☐ Safeguarding concern identified	☐ Other: _____	6. PEOPLE NOTIFIED Headteacher notified by: _____ Time: _____ DSL notified by: _____ Time: _____ DL Solutions notified by: _____ Time: _____ Lee Precious informed: ☐ Yes ☐ No	7. POTENTIAL IMPACT ASSESSMENT (tick all that apply) <table><tr><td>☐ No immediate impact identified</td></tr><tr><td>☐ Temporary system disruption</td></tr><tr><td>☐ Loss of access to systems</td></tr><tr><td>☐ Potential data breach</td></tr><tr><td>☐ Confirmed data breach</td></tr><tr><td>☐ Potential safeguarding implications</td></tr><tr><td>☐ Confirmed safeguarding implications</td></tr><tr><td>☐ Financial risk identified</td></tr><tr><td>☐ Reputational risk identified</td></tr></table>	☐ No immediate impact identified	☐ Temporary system disruption	☐ Loss of access to systems	☐ Potential data breach	☐ Confirmed data breach	☐ Potential safeguarding implications	☐ Confirmed safeguarding implications	☐ Financial risk identified	☐ Reputational risk identified
☐ Device disconnected from network																						
☐ Password reset																						
☐ MFA reset																						
☐ Device powered down																						
☐ Email quarantined / deleted																						
☐ User account disabled																						
☐ DL Solutions informed																						
☐ Headteacher informed																						
☐ DSL informed																						
☐ Safeguarding concern identified																						
☐ Other: _____																						
☐ No immediate impact identified																						
☐ Temporary system disruption																						
☐ Loss of access to systems																						
☐ Potential data breach																						
☐ Confirmed data breach																						
☐ Potential safeguarding implications																						
☐ Confirmed safeguarding implications																						
☐ Financial risk identified																						
☐ Reputational risk identified																						
8. INVESTIGATION OUTCOME _____ _____ _____ _____ _____	9. EXTERNAL AGENCIES CONTACTED <table><tr><td>☐ None required</td><td>☐ Local Authority</td></tr><tr><td>☐ ICO</td><td>☐ Data Protection Officer</td></tr><tr><td>☐ NCSC</td><td>☐ Other: _____</td></tr><tr><td>☐ Police</td><td></td></tr></table> Reference numbers (if applicable): _____	☐ None required	☐ Local Authority	☐ ICO	☐ Data Protection Officer	☐ NCSC	☐ Other: _____	☐ Police		10. RECOVERY ACTIONS COMPLETED (tick all that apply) <table><tr><td>☐ Passwords changed</td><td>☐ Staff informed</td></tr><tr><td>☐ Accounts secured</td><td>☐ Governors informed</td></tr><tr><td>☐ Devices scanned</td><td>☐ Parents informed (if applicable)</td></tr><tr><td>☐ Systems restored</td><td>☐ Additional filtering applied</td></tr><tr><td>☐ Data recovered from backup</td><td>☐ Additional training planned</td></tr></table>	☐ Passwords changed	☐ Staff informed	☐ Accounts secured	☐ Governors informed	☐ Devices scanned	☐ Parents informed (if applicable)	☐ Systems restored	☐ Additional filtering applied	☐ Data recovered from backup	☐ Additional training planned		
☐ None required	☐ Local Authority																					
☐ ICO	☐ Data Protection Officer																					
☐ NCSC	☐ Other: _____																					
☐ Police																						
☐ Passwords changed	☐ Staff informed																					
☐ Accounts secured	☐ Governors informed																					
☐ Devices scanned	☐ Parents informed (if applicable)																					
☐ Systems restored	☐ Additional filtering applied																					
☐ Data recovered from backup	☐ Additional training planned																					
11. LESSONS LEARNED / FOLLOW-UP ACTIONS _____ _____ _____																						
12. REVIEW Reviewed by: _____ Role: _____ Date reviewed: _____ Further action required? ☐ Yes ☐ No If yes, details: _____	13. SIGN OFF Headteacher: _____ Date: _____ DSL: _____ Date: _____ DL Solutions: _____ Date: _____																					

 Cyber security is everyone's responsibility.
If in doubt, report it.

 SAFEGUARDING
OUR CHILDREN

 PROTECTING
OUR INFORMATION

 SECURING OUR
SCHOOL SYSTEMS

Appendix 4 – Key Contacts

Headteacher: Alex Russ

DSL: Alex Russ

DDSLs: Jeanette Evans, Fiona Goodbrand, Lianne Steventon-Kiy, Louise Boroughs, Alex Keene

IT Support Provider: DL Solutions

Named Technician: Lee Precious

Governor Lead: Joel Tunbridge