Batchley First School Online Safety Policy

Date: November 2025
Review Date: November 2027
Policy Owner: Designated Safeguarding Lead

Contents

---

1. Policy Statement and Aims

1.1 Our Commitment

At Batchley First School we build in the use of these technologies to arm our pupils with the skills they need to access life-long learning. We aim to equip them with the knowledge they need to be safe and responsible while working both on and offline.

Computing and technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of both our pupils and staff. This policy creates and maintains a safe online and technological environment for our entire school community.

1.2 Policy Scope

This policy applies to:

- All pupils
- All teaching and non-teaching staff
- Governors
- Parents and carers
- Visitors, volunteers and contractors
- Anyone accessing school ICT systems and networks

1.3 Our Aims

We aim to:

- Provide a safe online environment where pupils can learn, explore and develop digital skills
- Educate pupils about online risks and how to stay safe
- Protect pupils from harmful and inappropriate online content, whilst teaching them about risks online, how to spot them and how to minimise the risk.
- Ensure staff understand their safeguarding responsibilities in relation to online safety
- Support parents and carers to keep children safe online at home
- Comply fully with Keeping Children Safe in Education (KCSIE) 2025 and all relevant legislation

1.4 Links to Other Policies

This policy should be read in conjunction with:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Policies (staff and pupils)
- Remote Learning Policy
- Image Use and Consent Policy

---

2. Roles and Responsibilities

2.1 Governing Body

The governing body will:

- Ensure the school has appropriate filtering and monitoring systems in place
- Review this policy annually and ensure it reflects current risks and guidance
- Ensure online safety is a standing item on the safeguarding governor's agenda
- Receive regular reports on online safety incidents and trends
- Ensure appropriate resources and training are allocated to online safety

Link Governor for Online Safety: S Heighway

2.2 Headteacher

Mrs Sarah Downes will:

- Ensure this policy is implemented effectively
- Ensure staff receive appropriate online safety training
- Ensure online safety is embedded across the curriculum
- Take overall responsibility for data and data security
- Ensure the school meets its statutory duties under KCSIE 2025

2.3 Designated Safeguarding Lead (DSL)

Mrs Lisa Brough (Safeguarding Lead) will:

- Take lead responsibility for online safety
- Oversee all online safety concerns and incidents
- Ensure online safety is integrated into safeguarding procedures
- Liaise with external agencies regarding online safety concerns
- Provide regular reports to the Headteacher and governors
- Keep up to date with emerging online risks and trends
- Ensure all safeguarding concerns with an online element are recorded on MyConcern

Deputy DSLs: Sarah Downes, Justine Fitzer and Alun Reeves

2.4 Online Safety Coordinators

Mr Alun Reeves (Deputy Headteacher) and **Mrs Kelly Foster (Computing Coordinator)** will:

- Support the DSL in promoting online safety across the school
- Coordinate online safety education within the curriculum
- Oversee technical aspects of filtering and monitoring
- Provide advice and support to staff on online safety matters
- Maintain and update online safety resources

- Monitor the effectiveness of filtering and monitoring systems
- Review online safety incidents and identify trends

2.5 All Staff

All staff must:

- Read and adhere to this policy and the Staff Acceptable Use Policy
- Model safe and responsible use of technology
- Embed online safety messages in their teaching
- Be alert to signs of online abuse or concerning behaviour
- Report any online safety concerns immediately to the DSL
- Attend annual online safety and safeguarding training
- Maintain appropriate professional boundaries in all online communications
- Never use personal devices to contact pupils or parents

2.6 IT Technician (Bordesley ICT)

Our IT technician will:

- Maintain the technical security of our school ICT systems
- Ensure filtering and monitoring systems are effective and regularly reviewed
- Support with the investigation of online safety incidents
- Ensure software and systems are kept up to date
- Provide technical advice on online safety measures
- Report any concerns about system security to the Headteacher

2.7 Pupils

Pupils are responsible for:

- Reading and following the Pupil Acceptable Use Agreement
- Using technology safely and respectfully
- Keeping passwords secure and not sharing login details
- Reporting any online safety concerns to a trusted adult
- Being kind and respectful in all online communications
- Understanding that online actions have real-world consequences

2.8 Parents and Carers

Parents and carers are responsible for:

- Supporting the school's online safety approaches

- Discussing online safety with their children at home
- Supervising their children's use of technology outside school
- Reporting concerns about online safety to the school
- Setting appropriate parental controls on home devices
- Following the school's social media guidelines

---

3. Education and Curriculum

3.1 Online Safety Education for Pupils

Online safety lessons are integrated into each year group's learning roadmap. The sessions are linked to the Project Evolve tool kit.

Our online safety curriculum covers:

Foundation Stage and Key Stage 1:

- How to use technology safely and respectfully
- Keeping personal information private
- Who to talk to if something online makes them feel worried or upset
- Being kind online
- Understanding that not everything online is true
- Recognising that people online might not be who they say they are

Key Stage 2:

- Understanding different types of online risks (content, contact, conduct, commerce)
- Critical evaluation of online information and content
- Managing online relationships and recognising unhealthy behaviour
- Understanding digital footprints and online reputation
- Recognising and responding to cyberbullying
- Understanding the risks of sharing images online
- Recognising grooming and exploitation
- Understanding age restrictions on apps, games and social media
- Reporting mechanisms (CEOP button, trusted adults, Childline)
- Respectful online communication
- Copyright and ownership of online content
- Safe and responsible use of AI

3.2 Age-Appropriate Teaching

We ensure online safety education is age-appropriate and tailored to pupils' needs:

- **Nursery and Reception:** Focus on basic rules, kind behaviour, and talking to trusted adults
- **Years 1-2:** Building understanding of online risks through stories, role-play and discussions
- **Years 3-4:** Developing critical thinking skills and understanding of more complex online scenarios
- **Year 4:** Preparing for transition to middle school with emphasis on social media risks, peer pressure, and maintaining positive online relationships

3.3 Curriculum Integration

As part of the Computing curriculum, all pupils will have digital literacy sessions and assemblies that focus on different elements of staying safe online. These sessions include topics such as, how to use a search engine, digital footprints, personal data protection, and cyberbullying. We also take part in Safer Internet day following their chosen theme.

Online safety is also embedded across the curriculum including:

- **PSHE:** Relationships, health and wellbeing, including online relationships
- **Computing:** Technical skills alongside safety awareness
- **English:** Critical literacy skills when reading online content
- **Assemblies:** Regular whole-school messages about staying safe online

3.4 Responding to Emerging Risks

We regularly review and update our curriculum to address:

- New platforms, apps and technologies popular with children
- Emerging online threats and trends
- Current safeguarding concerns highlighted in local and national data
- Feedback from pupils, parents and staff about online safety concerns

3.5 Artificial Intelligence (AI) and Emerging Technologies

We educate pupils about:

- What AI is and how it works in age-appropriate terms
- Benefits and risks of AI tools (chatbots, image generators, etc.)
- How to identify AI-generated content
- Understanding that AI can produce inaccurate or inappropriate content
- Appropriate and inappropriate uses of AI in their learning

- The importance of critical thinking when using AI tools

3.6 Gaming and Live Streaming

We recognise that many primary-age children engage with gaming and live streaming platforms. Our education includes:

- Understanding risks in gaming environments (chat functions, in-game purchases, contact with strangers)
- Recognising inappropriate content in games
- Understanding age ratings (PEGI) and why they matter
- Risks of live streaming platforms (YouTube, TikTok, etc.)
- Privacy settings and how to use them
- Not sharing personal information in gaming or streaming contexts

---

4. Acceptable Use of Technology

4.1 Pupil Acceptable Use

Email: Pupils are provided with a school email address that is accessed via our online learning environment (Office 365). The email section of their account is not accessed until KS2 where pupils are thought how to use the email facilities within school safely and responsibly.

All email use must follow these rules:

- Pupils do not have access to e-mail except in teacher-controlled situations.
- Pupils do not read e-mail messages from a non-school address unless an adult is present, or the messages have been reviewed by the teacher.
- Pupils never send an e-mail message to a person outside of the school network without having the contents approved by their teacher.
- Pupils must use appropriate, respectful language in all emails
- Pupils must report any concerning or inappropriate emails immediately

Cloud Storage (Office 365): All staff and pupils are provided with an Office 365 account. Documents and emails are accessed securely via login. Each account has access to a personal storage account for The Cloud.

Pupils must:

- Keep their login detail safe and secure
- Never share passwords with anyone except parents and staff
- Only access their own account
- Use cloud storage for learning purposes only
- Understand that all online use is monitored

Internet Use: The school's Internet access will be designed for pupil and staff use including appropriate content filtering.

Pupils must:

- Be given clear objectives for Internet use and taught what use is acceptable and what is not
- Only access websites approved by staff
- Never deliberately search for inappropriate content
- Report any inappropriate content immediately
- Be critically aware of the materials/content they access online and are guided to validate the accuracy of information
- Understand that internet history is monitored

Digital Devices:

- Pupils may not have or use their own personal devices in school
- Pupils will not use digital cameras or video equipment at school unless specifically authorized by staff
- Pupils must handle all school devices with care
- Chromebooks and laptops must be carried horizontally with thumbs on top
- Devices must never be used near food or drink

4.2 Staff Acceptable Use

All staff must sign and adhere to the Staff Acceptable Use Agreement which includes:

General Principles:

- Teacher use of the iPad falls under the School's Acceptable Use of ICT Policy for Staff, the staff code of conduct, its Child Protection Policy and the Batchley iPad Staff Acceptable Use Policy
- All devices must be used for educational purposes only when in school
- Staff must maintain professional boundaries in all online communications
- Staff must not use personal social media accounts to contact pupils or parents
- Staff must model safe and responsible use of technology

Personal Devices:

- Staff and visitors may have personal mobile phones in school however, they must be switched off and away while working with the children
- If a member of staff has a particular reason for having their personal mobile phone with them, they must inform a member of SLT and make all staff in the area aware

- Staff may not use personal devices to take photographs of the children in school or whilst on a school trip
- Staff should always use the school phone(s) to contact parents, but where needed hide Caller ID if an emergency deems it necessary to use a personal phone.
- Staff may use their mobile phones in the staffroom/one of the school offices
- Staff can connect personal devices to the school wifi, if this is necessary.
- Smart watches must be set to 'do not disturb' or similar when working with children

School-Issued Devices (iPads, MacBooks, Chromebooks):

Staff must:

- Ensure devices are charged when needed.
- Keep their iPad in a safe place at all times when not being used.
- Keep the four-digit security PIN on their iPads confidential
- Report loss, theft or damage to the head teacher or Kelly Foster immediately
- Back up data securely by ensuring iCloud is enabled at all times
- Back up data to their own One Drive space. Never store data to the device Batchley MacBook and Chromebook

Staff must not:

- Modify the settings of their iPads in any way unless instructed by the commuting technicians
- Apply any permanent marks, decorations or modifications to their iPads
- Login to personal accounts such as social media, personal email accounts, personal online banking or online shopping
- Remove devices from protective cases unnecessarily
- Take devices off-site without permission from SLT

Photography and Cameras:

- Staff should always use a school camera to capture images and should not use their personal devices
- Images must only be taken for educational or safeguarding purposes
- Images must be stored securely on school systems only
- Images must be deleted when no longer needed in line with our retention schedule
- Staff must follow the Image Use and Consent Policy at all times

Passwords and Security:

- Staff must use strong passwords and change them regularly

- Passwords must never be shared with anyone
- Staff must never allow pupils to use their login credentials
- Staff must log out of systems when not in use
- Staff must report any security concerns immediately

Professional Conduct Online:

- Staff must maintain professional boundaries in all online communications
- Staff must not accept friend requests from current pupils or parents on personal social media
- Staff must not discuss pupils, parents or the school on social media
- Staff must report any inappropriate contact from pupils or parents online
- Staff must be aware that their online presence reflects on the school

4.3 Visitor and Volunteer Acceptable Use

All visitors, volunteers and contractors must:

- Sign in and be made aware of this policy if using technology in school
- Hand in mobile phones at reception or keep them switched off and out of sight at all times
- Never take photographs or videos of pupils without explicit permission from the Headteacher
- Not connect personal devices to the school network, unless granted permission to do so
- Follow all staff guidelines regarding technology use when in school
- Report any online safety concerns to a member of staff immediately
- Understand that failure to comply may result in their visit being terminated

Specific protocols for contractors:

- Contractors working on site must be briefed on mobile phone and photography policies
- If contractors need to use devices for work purposes, this must be agreed in advance with the Headteacher
- Contractors must work in areas away from pupils where possible
- Any contractor found using devices inappropriately will be asked to leave immediately

---

5. Filtering, Monitoring and IT Security

5.1 Filtering Systems

The school's Internet access will be designed for pupil and staff use including appropriate content filtering. This is monitored via Lisa Brough.

Our filtering system:

- Uses an Internet Service Provider who offers protection through the use of a 'walled garden' – currently, Smoothwall.
- Filters sites by a site grading process
- Filters sites by language content with prohibition of sites with unacceptable vocabulary
- Is provided and maintained by Bordesley ICT
- Blocks access to illegal content including child sexual abuse images, terrorist content, and extreme pornography
- Blocks access to age-inappropriate content including pornography, violence, and hate speech
- Allows educational content while protecting pupils from harmful material

5.2 How Filtering Decisions Are Made

Filtering decisions are made by:

- The DSL (Mrs Lisa Brough) in consultation with the Headteacher
- The IT technician (Bordesley ICT) for technical implementation
- The Online Safety Coordinators (Mr Alun Reeves and Mrs Kelly Foster)

We consider:

- Age-appropriateness of content for primary pupils
- Educational value versus risk
- Current safeguarding concerns and emerging threats
- Feedback from staff about blocked content that should be accessible
- KCSIE 2025 requirements and DfE filtering standards

5.3 Monitoring Systems

All online use is monitored via Senso. Lisa Brough and Alun Reeves (DSL and deputy) monitor use. Bordesley ICT technicians maintain the technical monitoring systems.

Our monitoring includes:

- Real-time monitoring of internet activity through Senso
- Flagging of concerning searches or content access
- Review of user activity logs
- Email screening for inappropriate content or contacts
- Monitoring of cloud storage and shared files

What is monitored:

- All internet searches and websites visited
- Any typed content, in any format.
- Email content (both sent and received)
- File sharing and cloud storage activity
- Login attempts and account access
- Downloads and uploads

5.4 Review Schedule

We review our filtering and monitoring systems:

- **Termly:** Full review of filtering effectiveness by DSL, Headteacher, and IT technician
- **Monthly:** Review of monitoring reports and any concerning activity
- **Weekly:** Quick check of flagged incidents by DSL / Deputy
- **Immediately:** When new risks emerge or incidents occur
- **Annually:** Full audit as part of policy review

5.5 Balancing Filtering with Education

We recognise that:

- Over-blocking can prevent access to legitimate educational content
- Pupils need to learn how to navigate the internet safely, not just be protected by filters
- Critical thinking and digital literacy are essential skills

Therefore we:

- Teach pupils why content is filtered and how to stay safe
- Allow supervised access to age-appropriate content for educational purposes
- Use "teachable moments" when inappropriate content is accidentally accessed
- Encourage pupils to report blocked content they need for learning
- Review and adjust filtering based on educational needs

5.6 Escalation Procedures

When concerning activity is detected:

Level 1 - Minor concerns (e.g., accidental access to blocked content):

- Staff member addresses immediately with pupil
- Reminder of acceptable use rules
- No further action if isolated incident

Level 2 - Moderate concerns (e.g., deliberate attempts to bypass filters):

- Immediate report to DSL
- Contact parents same day, if deemed appropriate
- Log on MyConcern
- Investigation by DSL and IT technician
- Sanctions as per behaviour policy
- May involve temporary loss of technology access

Level 3 - Serious concerns (e.g., accessing illegal content, evidence of grooming):

- Immediate report to DSL
- Headteacher informed immediately
- Log on MyConcern with full details
- Contact parents/carers
- May involve police referral
- May involve Children's Social Care referral
- Device may be seized as evidence
- Full investigation conducted
- Support plan put in place

5.7 IT Security

System security measures:

- Virus protection installed and updated regularly
- Firewalls maintained by Bordesley ICT
- Regular security patches and updates
- Secure password policies enforced
- Two-factor authentication where possible
- Regular backups of all data
- Secure disposal of old equipment

Staff responsibilities:

- Use strong, unique passwords
- Never share login credentials
- Log out when leaving devices unattended
- Report any security concerns immediately

- Do not attempt to bypass security measures
- Keep software up to date
- Be vigilant for phishing attempts

Pupil responsibilities:

- Keep passwords secret
- Never share login details
- Report any security concerns to staff
- Do not attempt to access other users' accounts
- Log out after use

5.8 Data Protection and Security

All data is protected in accordance with:

- UK GDPR and Data Protection Act 2018
- Our Data Protection Policy
- Information Commissioner's Office (ICO) guidance

We ensure:

- Personal data is stored securely
- Access is restricted to those who need it
- Data is only kept as long as necessary
- Secure deletion when no longer needed
- Regular audits of data security
- Staff training on data protection

5.9 Cyber Security

We follow guidance from:

- National Cyber Security Centre (NCSC)
- DfE Cyber Security Standards for Schools
- National Education Network

We have procedures for:

- Preventing cyber-attacks
- Detecting security breaches
- Responding to incidents
- Recovering from attacks

- Reporting to relevant authorities

In the event of a cyber-attack:

1. Isolate affected systems immediately
2. Contact Bordesley ICT technician
3. Inform Headteacher and DSL
4. Assess extent of breach
5. Report to ICO if personal data compromised
6. Inform affected parties as required
7. Implement recovery procedures
8. Review and improve security measures

---

6. Mobile Devices and Personal Technology

6.1 Staff Mobile Phones and Devices

Staff and visitors may have personal mobile phones in school however, they must be switched off and away while working with the children. If a member of staff has a particular reason for having their personal mobile phone with them, they must contact SLT and make all staff in the area aware.

Permitted use:

- Staff may use their mobile phones in the staffroom/one of the school offices
- On trips staff mobiles are used for emergency only
- If emergency contact is needed, staff should hide Caller ID when using personal phones

Prohibited use:

- Using mobile phones in classrooms or around pupils
- Taking photos or videos of pupils on personal devices
- Contacting parents via personal devices
- Using personal devices for school business

Consequences of breach:

- First breach: Verbal warning and reminder of policy
- Second breach: Written warning
- Serious or repeated breaches: Disciplinary action up to and including dismissal

6.2 Smart Watches and Wearable Technology

Staff:

- Smart watches must be set to 'do not disturb' or similar when working with children
- No photos or recordings to be taken on smart watches
- Notifications should be disabled during teaching time
- If smart watches cause distraction, staff may be asked to remove them

Pupils:

- Pupils are not permitted to wear smart watches in school
- If a pupil brings a smart watch to school, it must be handed to the office
- Parents will be contacted to collect the device

6.3 School Trips and Off-Site Visits

Staff mobile phone use on trips:

- One designated staff member should have a school device
- Personal mobiles may be carried for emergencies
- Photos must only be taken on school devices
- Staff must not use personal phones around pupils
- Emergency contact with parents should use school phone (via office) or hide caller ID

Pupil devices on trips:

- Pupils must not bring personal devices on school trips
- School will provide devices if needed for educational purposes
- Parents will be informed of this rule in trip letters

6.4 Visitors and Contractors

All visitors must:

- Be informed of mobile phone policy on arrival
- Hand in mobile phones at reception OR keep them switched off and out of sight
- Never take photos or videos of pupils
- Not use devices in areas where pupils are present

Contractors on site:

- Must be briefed on mobile phone policy before starting work
- If devices needed for work purposes, this must be agreed with Headteacher in advance
- Should work in areas away from pupils where possible
- Will be supervised if working in areas with pupil access
- Any breach will result in immediate removal from site

6.5 Parents and Carers

At school events:

- Parents and carers are permitted to take photos/videos of their children in school events
- They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner
- Parents must not take photos of other children without permission
- The Governing body may ban the use of photographic equipment by anyone who does not follow the school policy

At drop-off and pick-up:

- Parents should not use mobile phones in classrooms
- Photos should not be taken in school buildings or playgrounds without permission
- Parents should respect other families' privacy

---

7. Images, Photography and Video

7.1 Consent and Permissions

Annual consent process:

- Parents complete image consent forms at the start of each academic year (or on admission)
- Consent covers: school website, social media, newsletters, displays, local press and prospectus
- Parents can withdraw consent at any time by contacting the school office
- Class teachers maintain records of which pupils have/don't have consent in their pastoral care files
- Office maintains central record of all consents

What we ask consent for:

- Photographs on school website
- Photographs on school social media accounts
- Photographs in school newsletters
- Photographs in local press/media
- Video recordings of school events

- Photographs in classroom and corridor displays

Pupils without consent:

- Are not included in photographs where possible
- Are positioned out of shot for group photos
- Have faces blurred or covered if accidentally included
- Are not named in any captions or descriptions

7.2 Taking Images - Staff Guidance

Staff should always use a school camera to capture images and should not use their personal devices.

Appropriate images:

- Children fully clothed
- Appropriate activities and contexts
- Focus on the activity, not individual children where possible
- Group shots rather than close-ups of individuals
- Images that celebrate achievement and learning

Inappropriate images:

- Children in states of undress (e.g., changing for PE)
- Images that could be misinterpreted
- Close-ups that could identify children without consent
- Images taken in toilets or changing areas
- Images of distressed or upset children

When taking images, staff should:

- Only take images for educational or safeguarding purposes
- Consider whether the image is necessary
- Think about how the image could be perceived
- Ensure children are appropriately dressed
- Focus on groups rather than individuals where possible
- Be mindful of children without consent

7.3 Storage and Deletion

Photos taken by the school are subject to the Data Protection Act.

Storage requirements:

- All images must be stored on school systems only (Office 365, SharePoint)
- Images must not be stored on personal devices
- Images must not be taken home on USB drives or other portable media
- Access to stored images is restricted to staff who need it
- Images are backed up securely

Retention schedule:

- Curriculum images: Kept for current academic year plus one year
- Celebration images (website/displays): Kept for two years
- Safeguarding images: Kept in line with safeguarding records retention
- Marketing images: Kept for three years with ongoing consent
- Images deleted securely when no longer needed

When pupils leave:

- Images of pupils who leave are reviewed
- Images removed from displays and website where appropriate
- Consent is no longer valid once pupil leaves
- Images may be retained for archival purposes with ongoing consent

7.4 Use Across Different Platforms

School website:

- Pupils' full names will not be used in association with photographs
- Only first names or "pupils from Year X" used
- Images regularly reviewed and updated
- Old images removed when no longer relevant

Social media:

- School social media accounts managed by designated staff only
- Same consent and naming rules as website
- Comments monitored and inappropriate comments removed
- Privacy settings set to maximum

Newsletters:

- Consent checked before publication
- Names used only with specific permission
- Digital newsletters have same protections as website

Displays:

- Consent checked before creating displays
- Displays in public areas (reception) use only consented images
- Displays in classrooms may include more images as visitors are supervised
- Displays updated regularly and old images removed

Local press/media:

- Additional specific consent sought for press releases
- Parents contacted before images submitted to press
- Right to withdraw consent before publication

7.5 Third-Party Photographers

School photographers:

- Must have enhanced DBS check
- Must follow our image use policy
- Must not take images of pupils without consent
- Must provide secure ordering system for parents
- Must delete images after specified period
- Contract must include data protection clauses

Other photographers (e.g., at events):

- Must be briefed on school policy
- Must be supervised at all times
- Must not have unsupervised access to pupils
- Images must be reviewed before use

7.6 Parents Taking Photos at Events

Parents and carers are permitted to take photos/videos of their children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

Guidelines for parents:

- Photos are for personal use only
- Do not share images of other children on social media
- Do not take photos if asked not to by staff
- Respect other families' wishes regarding photography
- Do not take photos in changing areas or toilets

Events where photography may be restricted:

- When pupils without consent are performing
- Swimming galas or sports events where children are in swimwear
- Sensitive performances or activities
- When safeguarding concerns exist

---

8. Social Media and Online Communication

8.1 School Social Media Accounts

Official school accounts:

- School has official accounts on: Facebook
- Accounts are managed by: School office staff and Alun Reeves (deputy headteacher)
- All posts must be approved by Headteacher or Deputy Head before publishing
- Accounts are monitored daily for comments and messages

Content guidelines:

- Posts celebrate pupil achievement and school life
- Images follow consent and naming rules
- No personal information about pupils shared
- Professional tone maintained at all times
- No political or controversial content
- Regular posts to keep community engaged

Comment moderation:

- Comments are monitored regularly
- Inappropriate comments are hidden/deleted immediately
- Serious concerns are reported to DSL
- Parents making inappropriate comments may be blocked
- Persistent issues may result in police involvement

Privacy settings:

- Maximum privacy settings applied
- Only approved followers can see content where possible
- Regular review of followers/connections
- Suspicious accounts blocked

8.2 Staff Personal Social Media

Professional boundaries:

- Staff must not accept friend requests from current pupils or parents on personal social media
- Staff must not discuss pupils, parents or the school on social media
- Staff must not post anything that could bring the school into disrepute
- Staff should consider their online presence reflects on the school
- Staff should use privacy settings on personal accounts

Acceptable use:

- Staff may follow official school accounts
- Staff may share official school posts
- Staff may mention working at the school in general terms
- Staff should maintain professional boundaries at all times

Unacceptable use:

- Posting about pupils, parents or colleagues
- Posting negative comments about the school
- Sharing confidential information
- Posting inappropriate content (even on private accounts)
- Contacting pupils

Consequences of breach:

- Minor breach: Verbal warning and reminder of policy
- Moderate breach: Written warning and social media training
- Serious breach: Formal disciplinary action
- Gross misconduct: May result in dismissal
- All breaches logged and may be referred to Teaching Regulation Agency if appropriate

Guidance for staff:

- Think before you post - would you be happy for pupils, parents or the Headteacher to see it?
- Use privacy settings but remember nothing online is truly private
- Be aware that screenshots can be taken and shared
- Consider having separate professional and personal accounts
- Never post when emotional or under the influence of alcohol

- Remember you are a role model for children

8.3 Responding to Negative Comments About School Online

If staff become aware of negative or defamatory comments:

1. Do not respond or engage with the comment
2. Take a screenshot as evidence
3. Report immediately to the Headteacher
4. Do not share or discuss with other staff
5. Allow senior leaders to handle the situation

School response to negative comments:

- Headteacher will assess the seriousness of the comment
- May respond professionally to correct misinformation
- May contact the parent/person directly to resolve
- May report to social media platform for removal
- May seek legal advice for defamatory or threatening comments
- May involve police if threats or harassment occur

Parents, pupils and staff will be advised that:

- Discussing pupils, staff or the school on social networking sites is inappropriate
- Defamatory comments may result in legal action
- Cyberbullying of staff or pupils will not be tolerated
- Concerns should be raised through proper channels (see complaints policy)

8.4 Communication Between Staff and Parents Online

Acceptable communication:

- Via official school email addresses only
- Through school communication platforms (e.g., Class Dojo, MCAS app)
- Via official school social media accounts
- During reasonable hours (8am-6pm on school days)

Unacceptable communication:

- Via personal email addresses
- Via personal social media accounts
- Via personal mobile phones (except emergencies on trips)
- Via messaging apps (WhatsApp, Messenger, etc.)

- Outside reasonable hours unless emergency

Staff should:

- Maintain professional boundaries at all times
- Keep communications professional and focused on the child's education
- Copy in another staff member if concerned about a communication (either cc or bcc)
- Report any inappropriate contact from parents to senior leaders
- Not share personal contact details with parents

8.5 Pupils and Social Media

School position:

- Use of social networking Internet sites (Facebook, Twitter, Instagram, TikTok, etc.) in school is not allowed and will be blocked/filtered
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils as most social media platforms have a minimum age of 13

Education for pupils:

- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location
- This includes not using personal photographs and videos
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others
- Pupils are taught about the risks of social media through our online safety curriculum
- Pupils are taught what to do if they encounter problems online

If pupils are using social media outside school:

- Parents are responsible for supervision and monitoring
- School will provide guidance and resources for parents
- School will address any issues that arise from out-of-school social media use if it affects the school community
- Cyberbullying incidents will be dealt with under our behaviour and anti-bullying policies

---

9. Safeguarding and Online Risks

9.1 Overview

This section outlines specific online safeguarding risks that staff must be aware of and how to respond. All staff must be alert to these risks and report any concerns immediately to the DSL.

9.2 Child Sexual Exploitation (CSE) and Online Grooming

What it is:

- Adults building relationships with children online to sexually abuse them
- May involve gifts, attention, or promises
- May progress to requests for sexual images or meetings
- Can happen on social media, gaming platforms, or any online space

Indicators staff should look for:

- Pupil talking about new online friends, especially adults
- Secretive behaviour around devices
- Receiving gifts or money from unknown sources
- Sexualised language or behaviour
- Unexplained access to money or new possessions
- Changes in behaviour, mood, or attendance

How we respond:

- Immediate referral to DSL
- DSL will assess and may refer to Children's Social Care
- May involve police if criminal activity suspected
- Support plan put in place for the child
- Parents informed unless this would place child at greater risk
- Education for all pupils about grooming and how to stay safe

9.3 Child Criminal Exploitation (CCE)

What it is:

- Children being exploited to commit crimes
- May include county lines drug dealing
- Online recruitment and communication
- Coercion and control often involved

Online elements:

- Recruitment through social media
- Communication via encrypted messaging apps
- Instructions given online
- Threats and intimidation via online platforms

- Images/videos used for blackmail

Indicators staff should look for:

- Unexplained money, clothes, or devices
- Going missing from school or home
- Decline in school performance
- New friendships with older individuals
- Secretive about online activity
- Signs of physical harm
- Carrying weapons or drugs

How we respond:

- Immediate referral to DSL
- DSL will refer to Children's Social Care and police
- Multi-agency approach to safeguarding
- Support for the child as a victim
- Work with parents where appropriate
- Education about exploitation risks

9.4 Radicalisation and Extremism Online

What it is:

- Process by which people come to support terrorism and extremism
- May lead to involvement in terrorist activities
- Online content can radicalise vulnerable individuals
- Conspiracy theories can be a gateway to extremism

Online indicators:

- Accessing extremist content online
- Sharing extremist views or materials
- Changes in behaviour or appearance
- Isolating from previous friends
- Expressing feelings of grievance or injustice
- Glorifying violence
- Accessing conspiracy theory content that promotes harm

How we respond:

- Immediate referral to DSL
- DSL will refer to Channel programme (Prevent)
- Police involvement where appropriate
- Support plan for the child
- Work with family where appropriate
- Education about critical thinking and evaluating online content
- Teaching about British values and respect for diversity

9.5 Serious Violence

Online elements:

- Content promoting gang culture or violence
- Videos showing violent acts
- Music videos that incite violence
- Social media used to threaten or intimidate
- Online disputes that escalate to real-world violence

Indicators staff should look for:

- Accessing violent content online
- Sharing violent images or videos
- Talking about gangs or violence
- Changes in behaviour or friendship groups
- Unexplained injuries
- Carrying weapons
- Fear or anxiety about certain areas or people

How we respond:

- Immediate referral to DSL
- Assessment of risk to child and others
- May involve police and Children's Social Care
- Support plan including work on conflict resolution
- Education about consequences of violence
- Work with parents and community partners

9.6 Mental Health and Harmful Content

Types of harmful content:

- Self-harm content and encouragement
- Suicide content including methods and encouragement
- Pro-eating disorder content (pro-ana, pro-mia)
- Content promoting dangerous challenges
- Content promoting substance abuse

Indicators staff should look for:

- Changes in mood, behaviour, or appearance
- Withdrawal from friends and activities
- Accessing harmful content online
- Physical signs (weight loss, injuries)
- Talking about self-harm or suicide
- Expressing hopelessness or worthlessness
- Changes in eating habits

How we respond:

- Immediate referral to DSL
- DSL liaises with senior mental health lead
- Risk assessment completed
- May involve CAMHS or other mental health services
- Parents informed and involved
- Support plan put in place
- Education about mental health and where to get help
- Filtering reviewed to block harmful content where possible

9.7 Sexual Violence and Harassment Online

What it is:

- Unwanted sexual comments or requests online
- Sharing of sexual images without consent
- Sexual coercion or pressure online
- Upskirting (taking photos under clothing)
- Image-based abuse

How it manifests online:

- Sexual messages or comments on social media

- Requests for sexual images
- Sharing of sexual images without consent
- Creating fake profiles to harass someone
- Rating people's appearance online
- Sexual rumours spread online

How we respond:

- Immediate referral to DSL
- Taken seriously even if it seems minor
- Victim supported and never blamed
- Investigation conducted
- May involve police if criminal offence
- Perpetrator held accountable
- Education for all pupils about consent and respect
- Links to our behaviour and anti-bullying policies

9.8 Harmful Sexual Behaviour Online

What it is:

- Age-inappropriate sexual behaviour
- Accessing pornography
- Sharing sexual content
- Sexual conversations or role-play online
- Creating or sharing sexual images

For primary-age children this may include:

- Accessing pornography (often accidentally)
- Exposure to sexual content in games or apps
- Inappropriate sexual talk online
- Sharing inappropriate images (often not understanding the implications)

How we respond:

- Referral to DSL for assessment
- Consideration of whether behaviour is age-appropriate or concerning
- Discussion with parents
- Education about age-appropriate behaviour

- May involve Children's Social Care if significant concerns
- Support plan if needed
- Review of filtering to prevent access to inappropriate content

9.9 Upskirting and Image-Based Abuse

What it is:

- Taking photos under someone's clothing without consent
- Sharing intimate images without consent
- Creating fake intimate images
- Threatening to share intimate images (sextortion)

How we respond:

- Immediate referral to DSL
- This is a criminal offence - police will be involved
- Victim supported and never blamed
- Attempts made to remove images from circulation
- Perpetrator held accountable
- Education for all pupils about consent and the law
- Clear message that this is never acceptable

9.10 Modern Slavery and Trafficking

Online elements:

- Recruitment through social media
- Victims controlled through online communication
- Victims may be forced to work in online exploitation
- Trafficking networks use online platforms

Indicators staff should look for:

- Signs of physical abuse or neglect
- Fearful or anxious behaviour
- Lack of personal possessions
- Inappropriate clothing for weather
- Malnourished or unkempt appearance
- Not registered with GP or dentist
- Limited social interaction

- Signs of control by another person

How we respond:

- Immediate referral to DSL
- DSL will refer to Children's Social Care and police
- Modern Slavery Helpline contacted (0800 0121 700)
- Multi-agency approach to safeguarding
- Specialist support for the child
- Sensitive approach recognising child as victim

---

10. Peer-on-Peer Abuse

10.1 Overview

We recognise that children can abuse other children, and this can happen online as well as offline. All peer-on-peer abuse is unacceptable and will be taken seriously. Staff must not dismiss abusive behaviour as "just banter" or "part of growing up."

10.2 Cyberbullying

Definition: Cyberbullying is bullying that takes place online or through digital devices. It can include:

- Sending hurtful messages or emails
- Posting embarrassing photos or videos
- Spreading rumours online
- Creating fake profiles to humiliate someone
- Excluding someone from online groups
- Threatening or intimidating someone online

Why it's different from other bullying:

- Can happen 24/7
- Can reach a wide audience quickly
- Content can be permanent and difficult to remove
- Can be anonymous, making perpetrators feel less accountable
- Victim has no safe space if it follows them home

Prevention:

- Education about cyberbullying in online safety curriculum
- Clear message that cyberbullying is never acceptable

- Teaching about being an upstander not a bystander
- Promoting positive online behaviour and digital citizenship
- Regular assemblies and discussions about kindness online

How we respond:

- All reports of cyberbullying taken seriously
- Immediate referral to DSL or senior leader
- Investigation conducted promptly
- Evidence gathered (screenshots, etc.)
- Victim supported and reassured
- Parents of both victim and perpetrator informed
- Sanctions applied as per behaviour policy
- May involve police if criminal offence (threats, harassment)
- Support plan for both victim and perpetrator
- Follow-up to ensure bullying has stopped

Support for victims:

- Believed and taken seriously
- Reassured it's not their fault
- Helped to remove or report harmful content
- Taught strategies to stay safe online
- Ongoing monitoring and check-ins
- Access to counselling if needed
- Links to external support (Childline, etc.)

Work with perpetrators:

- Held accountable for their actions
- Helped to understand impact of their behaviour
- Education about empathy and consequences
- Sanctions appropriate to the severity
- Support to change behaviour
- Monitoring to prevent repeat incidents
- May involve external agencies if serious or persistent

10.3 Sharing of Nudes and Semi-Nudes

Important note: We use the term "sharing of nudes and semi-nudes" as recommended by KCSIE 2025. This was previously called "sexting." We do not use the term "sexting" as it can normalise the behaviour.

What it is:

- Creating, sharing, or possessing sexual images or videos of anyone under 18
- This is illegal even if the person in the image created and shared it themselves
- Includes images shared consensually between young people in relationships
- Includes images shared under pressure or coercion

Why children do it:

- Peer pressure
- Romantic relationships
- Bullying or coercion
- Attention seeking
- Not understanding the consequences
- Believing images will remain private

How we respond:

If a staff member becomes aware of an incident:

1. **Do not view, copy, print, or share the image** - this is illegal
2. Report immediately to the DSL
3. Confiscate the device if appropriate and secure it
4. Do not ask the child to show you the image
5. Reassure the child they have done the right thing by telling you

DSL response:

1. Assess the risk and context using UKCIS guidance "Sharing nudes and semi-nudes: advice for education settings"
2. Consider:
    - Ages of those involved
    - Whether there is a significant age gap
    - Whether the image was created/shared consensually
    - Whether anyone was coerced
    - Whether the image has been shared widely
    - Whether there are any safeguarding concerns

3. Decide whether to:
    - Handle internally with support and education
    - Involve parents
    - Refer to Children's Social Care
    - Refer to police

When we involve police:

- If there is evidence of exploitation or grooming
- If there is a significant age gap
- If images have been shared widely
- If there is evidence of coercion or blackmail
- If an adult is involved
- If there are other safeguarding concerns

When we may handle internally:

- Consensual sharing between peers of similar age
- No evidence of coercion or exploitation
- Image not shared widely
- No aggravating factors
- Appropriate education and support can be provided

In all cases:

- Victim is supported and never blamed
- Clear message that sharing images is illegal and harmful
- Education about consequences and how to stay safe
- Parents informed (unless this would put child at greater risk)
- Recorded on MyConcern
- Follow-up to ensure no repeat incidents

Prevention education:

- Age-appropriate education about relationships and consent
- Clear message about the law
- Discussion of consequences (legal, social, emotional)
- Teaching about pressure and how to resist it
- Emphasis on respecting yourself and others

- What to do if you're asked to share an image

10.4 Online Sexual Harassment

What it is:

- Unwanted sexual comments or jokes online
- Sexual rumours spread online
- Rating people's appearance online
- Unwanted sexual messages or images
- Sharing of sexual images without consent
- Pressure to engage in sexual activity online

How it manifests in primary schools:

- Inappropriate sexual language in online communications
- Sharing of sexual content (often from older siblings or online)
- Sexual comments about appearance
- Pressure to engage in sexual talk or role-play
- Exposure to pornography and sharing it

How we respond:

- All reports taken seriously, even if seems minor
- Immediate referral to DSL
- Investigation conducted
- Victim supported and never blamed
- Perpetrator held accountable
- Education about respect, consent, and appropriate behaviour
- Parents informed