

St Matthew's Bloxam C of E Primary School



Online Safety and Filtering and Monitoring Policy 2026

Purpose of Online Safety and Filtering and Monitoring Policy

This Online Safety and Filtering and Monitoring Policy has been created by St Matthew's Bloxam C of E Primary School teachers, governors and school councillors. The aim of the policy is to provide children, parents and staff with information on how the school will:

- Safeguard and protect children, staff and parents/carers.
- Educate and raise awareness of online safety throughout the school and local community;
- Manage professional standards and practice when using technology and Identify clear procedures when responding to online safety concerns.

Although considerable, the school outlines 3 significant areas of risk:

- 1) Content – Being exposed to illegal / inappropriate materials
- 2) Contact – Being exposed to, and exposing others to, harmful online interaction
- 3) Conduct – Personal online behaviour which could lead to harm.

Why Internet use is important

- Internet access is an entitlement for all Children.
- Technology (computers, tablets, phones) is an important part of everyday life and an integral element in the 21st century for education, business and social interaction. School has a duty to provide children with quality internet access and it is part of the statutory curriculum and should be taught in order to develop a range of strategies to respond to risk online.
- Online safety issues are embedded in all aspects of the curriculum.

During computing sessions, teachers reference online safety where

appropriate. Internet use will enhance learning

- Children are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide Children in on-line activities that will support the learning outcomes planned for the children's age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Aims and Objectives

- To provide staff with the key information to deal with online safety issues in a safe and effective manner.
- To ensure that staff have the ability to deal with content, contact and conduct issues on line.
- To provide staff with a point of reference when dealing with online safety issues.

Equal Opportunities

- All children should have equal access to the use of the internet.
- Further information on equal opportunities and special needs is given in the relevant school policies.

Online Safety Curriculum

- Online safety should be a focus in all areas of the curriculum.
- Staff should reinforce online safety messages whenever Computing is used.
- Children will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Children will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- In lessons where internet use is pre-planned, it is best practice that Children should be guided to sites checked as suitable for their use. Processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, (e.g. using search engines) staff should not solely rely on the filtering system in place and be vigilant in monitoring the content of the websites the Children visit and provide close supervision.
- Children should be taught in all lessons to be critically aware of the materials

/ content they access on-line and be guided to validate the accuracy of information.

- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Early Years and Foundation Stage - Children are introduced to early online safety messages and take part in Online Safety Week. Any technology used in the classroom is overseen by staff.
- Key Stage 1 - Children should be taught to: use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Key Stage 2 - Children should be taught to: use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Pupils will be taught how to evaluate Internet content

- If staff or children discover unsuitable sites, which have slipped through the filtering system, the URL (address), time, date and content must be reported to the Designated Safeguarding Lead, who then must report it to Warwickshire ICT Development Service.
- The school will ensure that the use of Internet derived materials by staff and by children complies with copyright law.
- Children will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information System Security

- The security of the school information systems will be reviewed regularly.
- Virus protection formulates part of the Warwickshire County Council's IT system management for schools.

Infrastructure, system security, filtering and monitoring

- The Online Safety and Filtering and Monitoring Policy will be reviewed annually, after any serious incident or after any local/national policy requirements.
- Virus protection will be installed and updated after serious incidents.
- The school will work in partnership with the Warwickshire ICT Development Service for filtering and monitoring. All possible harmful reports will be highlighted to the Headteacher and Online Safety / Computing Lead.
- The school Internet access is designed expressly for pupil use and includes filtering and monitoring appropriate to the age of pupils by Smoothwall Filter

Solution, which is used by all school who subscribe to Warwickshire ICT Development Service. (WCC ICTDS). St Matthew's Bloxam C E Primary School is a subscribing school.

- This network monitors 45,000 staff and pupils across the county, including all staff and children at St Matthew's Bloxam C E Primary School. WCC ICTDS uses Smoothwall Filter Solution to provide monitoring and filtering for all of its schools. Subsequently, St Matthew's Bloxam C E Primary School uses this to ensure that all members of the school community are able access online material safely. Smoothwall blocks and proactively monitors harmful or dangerous content without over blocking, ensuring that students and staff are able to continue learning whilst safely explore the internet. These meet the Government Standards for Filtering and Monitoring 2023 and the requirements of Keeping Children Safe in Education 2025.
- The filtering and monitoring provision are managed by the school Designated Safeguarding Lead, in line with the school safeguarding policy and the Keeping Children Safe in Education 2025 (KCSiE) requirements, and is reviewed annually.
- The school works in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.
- If staff or Children discover unsuitable sites, the URL, time and date must be reported to the school Online Safety / Computing Lead, who will report this to the ICT Development Service filtering team and block it.

Internet Access

- All staff and children who are granted Internet access.
- All teachers and some wider office personal are allocated laptops and devices for school use. Staff are made aware that Internet use is monitored and traced to the individual user. All staff are made aware of the reference made to Online Safety in the Staff Code of Conduct Policy.
- Parents / Carers are requested to sign the 'Online Safety Agreement' form for parents/carers of Primary aged children' as part of the Home/School Agreement.
- Children sign the 'Online Safety Agreement' form for KS1 / KS2 school pupils.
- School visitors have access to the internet where necessary as this is controlled by a school-based password.

Internet Risks

- In common with other media, such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.
- The Computing Lead and Designated Safeguarding Leads will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Recording reported events on the school CPOMS system.
- The Headteacher ensures that the Online Safety Policy is implemented and compliance with the policy is monitored.

Assessing risks

- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of internet access.

E-mail

- Pupils use e-mail accounts on the school system for specific units of work within the Computing curriculum.
- All pupils are allocated a WeLearn365 account when they join the school. This is used to log onto computers and to access the programs used for teaching the curriculum. Every WeLearn account has an email address.
- The school also uses set class email addresses, used purely for communication of work during prolonged absence from school e.g. lockdowns, or for entries to class competitions or submitting particular tasks.

Social networking and personal publishing

- Children are taught about the safe use of social networking sites as part of their online safety lessons.
- Children are advised never to give out personal details of any kind which may identify them or their location. Any contact made by a stranger is turned off and reported to a parent, carer, teacher or adult of trust.
- Children and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged children, and that many social networking sites have a specified minimum age.

Learning Platforms, Virtual Learning Environments and other communication tools

- Children will be taught how to use communication tools appropriately, as part of general Computing lessons and online safety lessons.
- Children/staff will be advised on acceptable conduct and use when using communication tools.
- All users will be mindful of copyright issues and will only upload appropriate content.
- When staff, Children etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Username and passwords

- All children will be provided with a username and password in order to secure safe access to school curriculum devices, the learning platform and email. Children must use these when accessing school equipment.
- Children will be made aware that all technology will be monitored and be traced back to the individual user.
- Children in Foundation Stage will log on with a class account. Staff are aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy. Use by Children in this way should always be supervised by a member of staff.
- Staff should never use a class log on for their own network access.
Staff must:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Transfer data using encryption and secure password protected devices or one drive.

All Staff will be provided with a username and password, which will provide them secure access to school curriculum devices, the learning platform and email.

- Staff are provided with a username and password through the Warwickshire Learning Platform. Staff must use these when accessing school technology.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

Passwords

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy

- Logs are maintained of access by users and of their actions while users of the system
- A safe and secure username / password system is essential if the above is to be established and will apply to all school computer systems, including email and online learning websites.

Communication technologies:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education and considers it the benefits of their use in school outweighs their risks / disadvantages.

The school allows children to bring their mobile phones to school, for safety reasons, but insist that these are kept in the school office until home time.

The school, at times, permits the use of Blogs and Email where their use is linked to curriculum activities/learning.

The school does not permit the use of social networking, chat rooms or instant messaging.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official school email address should be used by parents/carers to communicate with staff members.

Authorising Internet access

- All staff must read and sign the school Acceptable Use Policy, before using any school ICT resource.
- Parents / Carers will be asked to sign and return a consent form in Reception or when a new student is registered.
- Staff will be made aware that all online use is monitored and understand the implications of misuse in line with the Acceptable Use Policy.

Data Protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff must:

- 1) Ensure the safe keeping of personal data.
- 2) Ensure that they use secure school technology and are securely logging off after each use.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- Use OneDrive as the preferred data storage in school.

Publishing and storing pupil images

- Photographs that include children will be selected carefully, and photographs of individual children will only be taken when relevant to particular events, activities or lessons.
- Children's full names will not be used anywhere on the website, learning platform, on school social media pages or stored within folders in the 'shared' or 'pupil shared' areas.

Responding to Incident of Misuse

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- Access to the communication tool for the user may be suspended for a period of time.
- The user will need to discuss the issues with a member of SLT before being permitted to use school technology again.
- A pupil's parent/carer may be informed.

Illegal activity:

It is hoped that all members of the school community will be responsible users of Computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Examples of illegal activity could include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials.

Inappropriate activity:

- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. Inappropriate use may result in a referral to the Online Safety Officer Refer, the Headteacher or to the Police.
- Sanctions for misuse may include, informing parents / carers, the removal of network / internet access rights.

Examples of misuse are as follows:

- Accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other handheld device
- Unauthorised use of social networking / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's / pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Staff inappropriate activity:

Examples of misuse are as follows:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g., holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
 - Accidentally accessing offensive or pornographic material and failing to report the incident
 - Deliberately accessing or trying to access offensive or pornographic material
 - Breaching copyright or licensing regulations
 - Continued infringements of the above, following previous warnings or sanctions.

Sexting and Sexual Imagery'

If the school is made aware of any incident involving sexting/sexual images involving a child we will:

Act in accordance with our child protection and Safeguarding policies and work closely with the police/local authority.

- Store the device securely.
- Immediately notify the DSL and Online Safety / Computing Lead.
- Block all online access to users (children and staff) and isolate the image if an indecent image has been shared on the Learning Platform.
- Carry out a risk assessment which considers any vulnerable children involved, including carrying out relevant checks with other agencies.
- Inform parents at an early stage, if appropriate, about the incident and how it is being managed.

- Make a referral to Specialist Children's Services/Police.

If a decision is made to view imagery the DSLs would need to be satisfied that viewing:

- Is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report.
- Is unavoidable because a child has presented an image directly to a staff member or the imagery has been found on a school device or network.

If it is necessary to view the imagery then the DSLs should:

- Never copy, print, save or share the imagery.
- Ensure viewing is undertaken by the DSL with at least 1 other member of the SLT.
- Ensure viewing takes place with another member of staff present in the room, ideally the Headteacher or a member of the senior leadership team. This staff member does not need to view the images.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the image.
- Keep a record of the viewing in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions.
- Ensure the record keeping is signed, dated and meets the wider standards set out by Ofsted for recording safeguarding incidents.

After every sexting or sexual image incident

Images will be deleted only once the school has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device (such as a mobile phone) has been seized, a teacher who has been formally authorised by the Headteacher can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved.

After every incident

The SLT and Online Safety / Computing Lead will review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures where necessary.

Recording incidents

All incidents relating to youth produced sexual imagery need to be recorded in school.

This includes incidents that have been referred to external agencies and those that have not.

Staff at St Matthew's Bloxam will record incidents in line with the above guidance.

Where we decide not to refer incidents to the police or children's social care, we will record the reason for doing so and ensure that this is signed off by the Headteacher.

Complaints and misuse

Complaints of internet misuse will be dealt with by the Headteacher.

If any apparent or actual misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials,

- The school will report the incident to the Local Authority in the first instance and inform the police.

Staff should refer to the Whistle Blowing Policy should they have complaints about a senior member of staff's use of the internet and feel they cannot approach the Headteacher. This can be found in the staff room or online.

Inappropriate usage by Children includes:

- Deliberately accessing or trying to access material that could be considered illegal.
- Deliberately accessing or trying to access material that is not age-appropriate.
- Unauthorized use of non-educational sites during lessons.
- Attempting to access or accessing the school network / Learning Platform using another user's account.
- Sending an email, text or other electronic message that is regarded as offensive, harassment or of a bullying nature.
- Actions which could bring the school into disrepute or breach the integrity or ethos of the school.

Staff, in line with the Positive Behaviour and Relationship Policy, will use one or more of the following sanctions depending on the severity of the misuse:

- Verbal
- Refer to the Online Safety / Computing Lead
- Refer to the Headteacher
- Inform parents / carers
- Remove network / internet access rights
- Refer to the police.

Inappropriate usage by Staff

Staff misuse of technology/internet is outlined in the school Code of Practice Staff Policy.

Depending on the seriousness of the inappropriate use by a member of staff, the Online Safety / Computing Lead / Headteacher may use one or more of the following sanctions:

- Refer to the Local Authority / ICT Development Service or HR
- Refer to Technical Support staff for action re: filtering
- Disciplinary action
- Refer to the police.

Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated at St Matthew's Bloxam.
- All incidents of cyberbullying reported to the school will be recorded along with the response and outcome.
- Children, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- All reported cases of cyberbullying will be recorded and investigated by the Online Safety / Computing Lead and/or Headteacher.

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers, from both parties, will be informed.
- The police will be contacted if a criminal offence is suspected.
- Ultimately a child could be excluded in line with the positive behaviour and relationship policy.

Preventing extremism and radicalisation

We know that extremists use the internet, including social media to share their messages. The filtering systems used at school block inappropriate content, including extremist content. Where staff, Children or visitors find unblocked extremist content they must report to the Online Safety / Computing Lead and Headteacher immediately – resulting in an immediate block of the website and a report being given to appropriate authorities.

If a pupil is found to be actively searching for extremist content, the DSLs must be informed so that they can take the appropriate action in line with the Preventing Extremism and Radicalisation Policy.

Using social media to engage/update parents and families

At St Matthew's Bloxam we aim to use as many different ways as possible including Facebook, Twitter to keep our parents and families up to date with what their children are doing and what is going on in school.

In line with The Online Safety and Filtering and Monitoring Policy:

- Access will be password protected.
- Only the operating class teacher/LSA will have access and must use school, password protected, equipment.

- Children, parents and visitors of St Matthew's Bloxam will not have access to class pages of other classes.

Writing and reviewing The Online Safety and Filtering and Monitoring Policy

- The Online Safety and Filtering and Monitoring Policy has been written by the Online Safety Coordinator in conjunction with governors and the headteacher.
- The Online Safety and Filtering and Monitoring Policy will be reviewed annually and compliance will be monitored throughout the year by the headteacher, Senior Leadership team and Online Safety / Computing Lead.

The Online Safety and Filtering and Monitoring Policy will be read and reviewed class teachers annually or after any serious incident.

Roles and Responsibilities

Governors:

- Governors are responsible for the approval of The Online Safety and Filtering and Monitoring Policy and for reviewing the effectiveness of the policy.
- A member of the Governing Body will attend Online Safety meetings and report back to other governors and attend relevant training.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety / Computing Lead where appropriate.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety / Computing Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues.

Online Safety Coordinator:

- Has overall day-to-day responsibility, Online safeguarding is discussed with the DSL and a plan of action is set up on an individual basis.
- Runs training for staff and parents.
- Reviews The Online Safety and Filtering and Monitoring Policy with other relevant members of staff yearly or after any serious incident – to ensure effectiveness.
- Keeps up to date with new risks, issues, developments and resources in the area of online safety.

Teaching and Support Staff:

- Read, understand and sign the school Staff Acceptable Use Policy / Agreement.
- Report any suspected misuse or problem to the Online Safety / Computing Lead /

Headteacher (and DSL) for investigation / action / sanction.

- Have an up to date awareness of online safety.
- Monitor ICT activity in lessons, extra-curricular and extended school activities.

Children:

- Are responsible for using the school ICT systems in accordance with the Pupil Online Safety Agreement.
- Should use their own user ID and password as appropriate.

Student Voice – School Councillors:

- Feedback on current concerns or online interests.

Parents / Carers:

- Will have the opportunity to attend an Online Safety workshop - date arranged and led by the Online Safety / Computing Lead.

Guests

- 'Guests' such as supply teachers are provided with a username and password if they require access to school systems.

This policy will be reviewed by the Resources Committee in the Autumn term 2027



Appendix 1

Part 1

Youth produced Sexual Imagery

Incidents Recording Sheet

<u>Date</u>	<u>Time imagery declared / discovered</u>
<u>Adults involved</u>	<u>Children involved</u>

Time reported to:

DSL_____

Head_____

Online Safety Coordinator_____

Details of Imagery

Next steps/agencies reported to

Adults involved from school & agency

Outcome

Any changes needed to policy/staff training & the adults that will monitor this.

--

Part 2

Viewed/deleted imagery record

Who initially decided the imagery need to be viewed or deleted?	
Which adults were involved in this decision? DSL Headteacher Senior leaders	
Why was the decision to view/delete taken? Please add as much detail as possible.	
Which adult viewed/deleted the imagery? When possible a same sex adult should view imagery.	
In which room did this take place? And with which adults in the same room at the time of viewing/deletion?	

Please complete part 1 and make sure the outcome of part 2 is recorded

