

King Athelstan Primary School

Online Safety Policy



King Athelstan Primary School - Inspiring Excellence

We believe in the relentless pursuit of excellence to achieve high standards.

We are driven to inspire our school community to be aspirational, ambitious and to "dream big."

We empower children with choices which prepare them for a life of opportunity.

We teach children that hard work delivers success; we encourage children to take risks and ask brilliant questions in order to inspire a love and passion for learning.

We teach children to think.

We put children's happiness and welfare at the heart of everything we do.

We value friendship, kindness and respect.

We celebrate the excellence in each individual.

We expect families to work with us to form a strong team around every child.

We teach children to be good citizens.

We are proud of our school: Come as you are and leave us great.

Responsibility: Computing Lead		Governors committee:	
Status: Not statutory or website		Review Cycle: Annual	
Date reviewed: June 2026	Date agreed:		Next review: June 2027

Contents

1. Aims	Error! Bookmark not defined.
2. Legislation and guidance.....	5
3. Roles and responsibilities	5
4. Educating pupils about online safety.....	12
5. Educating parents/carers about online safety	15
6. Cyber-bullying	15
7. Acceptable use of the internet in school	18
8. Managing Equipment and ICT Systems	19
9. Staff using work devices outside school.....	21
10. How the school will respond to issues of misuse.....	22
11. Training for staff, governors and volunteers	24
12. Monitoring arrangements.....	25
13. Links with other policies	25
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	Error! Bookmark not defined.
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)	Error! Bookmark not defined.
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	Error! Bookmark not defined.
Appendix 4: online safety training needs - self-audit for staff ..	Error! Bookmark not defined.
Appendix 5: online safety incident report log	Error! Bookmark not defined.

1. Aims:

King Athelstan Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Safeguard and protect all members of the school community when using digital technologies and online services, both within and beyond the school environment.
- Identify and support groups of pupils who may be at greater risk of harm online than others.
- Deliver an effective whole-school approach to online safety that empowers and educates pupils, staff, volunteers, governors and parents/carers in the safe and responsible use of technology, including mobile and smart technology (referred to in this policy as "mobile phones").
- Set out the key principles and expectations for the safe, responsible and appropriate use of digital technologies, communication systems and internet-based services by all members of the school community.
- Support staff in working safely, confidently and responsibly with the internet and other communication technologies, and in maintaining high standards of professional practice.
- Educate pupils to become safe, respectful and responsible digital citizens who can recognise, respond to and report online risks.
- Establish clear expectations for acceptable online behaviour and codes of practice for the educational, personal and recreational use of technology.
- Have clear structures and mechanisms to identify, report, respond to, intervene in and escalate online safety incidents where appropriate, including concerns such as cyberbullying, online abuse, harassment, exploitation and exposure to harmful content.
- Ensure that all members of the school community understand that unlawful, unsafe or inappropriate online behaviour is unacceptable and may result in disciplinary action and, where necessary, legal intervention.
- Minimise the risk of misplaced, malicious or inappropriate allegations made against adults working with pupils through the misuse of digital communication technologies.
- Promote a culture of vigilance, resilience, openness and accountability where online safety concerns can be discussed and addressed effectively.
- Ensure the school fulfils its statutory safeguarding, child protection and data protection responsibilities in relation to online safety.

The 4 Key Categories of Online Safety Risk

Our approach to online safety is based on addressing the following categories of risk:

Content

Being exposed to illegal, inappropriate or harmful content, including:

- Pornography
- Misinformation and disinformation (including fake news and conspiracy theories)
- Racist, misogynistic, antisemitic, extremist or hate-related content
- Content promoting self-harm, suicide, eating disorders or other harmful behaviours
- Radicalisation and extremism
- Lifestyle websites or online communities that promote unsafe or unhealthy behaviours
- Exposure to age-inappropriate or harmful material
- Understanding how to evaluate the authenticity, reliability and accuracy of online information and content

Contact

Being subjected to harmful online interaction with other users, including:

- Peer-to-peer pressure, coercion or intimidation
- Online bullying in all forms
- Commercial advertising and online manipulation
- Adults posing as children or young adults with the intention to groom, exploit or radicalise users
- Sexual, criminal, financial or other forms of exploitation
- Social or commercial identity theft, including misuse of passwords, accounts or personal information

Conduct

Personal online behaviour that increases the likelihood of, or causes, harm, including:

- Online bullying and aggressive or abusive behaviour
- Making, sending, receiving or sharing explicit images, including consensual and non-consensual sharing of nudes and semi-nudes
- Sharing pornography or other explicit content
- Privacy issues, including the disclosure of personal information
- Poor management of digital footprints and online reputation
- Unsafe, irresponsible or unlawful online behaviour
- Health and wellbeing concerns linked to technology use, including excessive screen time, online gambling and negative impacts on body image or mental health
- Copyright infringement and failure to respect intellectual property rights and ownership

Commerce

Risks linked to online commercial activity, including:

- Online gambling
- Phishing, scams and fraud
- Inappropriate advertising
- Financial exploitation or manipulation
- Unsafe in-app purchases or subscription services

Scope

This policy applies to all members of the King Athelstan community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school IT systems, both in and out of King Athelstan Primary School

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- > [Teaching online safety](#)
- > [Meeting digital and technology standards](#)
- > [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- > [Relationships and sex education \(RSE\) and health education](#) -
- > [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The governing body will ensure that the school has appropriate policies, procedures and practices in place to keep pupils, staff and the wider school community safe online.

The governing body will approve the Online Safety Policy and review its effectiveness regularly.

The governing body will support the school in encouraging parents/carers and the wider community to engage in online safety activities and awareness.

The governor who oversees online safety is Jess Castellino as Safeguarding Governor

The role of the online safety governor will include regular review of the online safety policy and liaison with the online safety co-ordinator and safeguarding leads.

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Acceptable use policy)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with special educational needs and/or disabilities (SEND), recognising that a "one size fits all" approach may not

be appropriate for all children and that a more personalised or contextualised approach may be required

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is implemented consistently throughout the school.

The headteacher will:

- Be appropriately trained in offline and online safeguarding, in line with statutory guidance and relevant safeguarding partnership guidance
- Lead a strong safeguarding culture in which online safety is fully integrated into the whole-school safeguarding approach
- Take overall responsibility for the provision and management of online safety across the school
- Take overall responsibility for data management and information security as the Senior Information Risk Owner (SIRO), ensuring the school follows best practice in information handling and data protection
- Ensure the school uses appropriate, secure and suitably filtered IT systems, networks and internet services
- Ensure that all staff receive suitable safeguarding and online safety training relevant to their roles and responsibilities
- Be aware of the procedures to be followed in the event of a serious online safety incident or allegation
- Ensure that appropriate risk assessments are undertaken so that the curriculum and wider school provision meet the needs of pupils, including identifying and addressing the risk of radicalisation and other online harms
- Ensure that effective systems are in place to monitor and support staff who carry out online safety responsibilities, including technical and network support staff
- Ensure governors are regularly updated on the nature, effectiveness and monitoring of the school's online safety arrangements
- Ensure that the school website includes relevant statutory information and appropriate online safety information for pupils, staff and parents/carers
- Work with the computing lead and safeguarding staff to address emerging online safety issues and ensure that the curriculum responds appropriately to new risks, trends or incidents through relevant teaching and learning opportunities

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding leads (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- › Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the headteacher and governing body to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly

- › Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- › Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- › Working with the ICT manager to make sure the appropriate systems and processes are in place
- › Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- › Managing all online safety issues and incidents in line with the school's child protection policy
- › Responding to safeguarding concerns identified by filtering and monitoring
- › Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- › Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- › Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- › Liaising with other agencies and/or external services if necessary
- › Providing regular reports on online safety in school to the headteacher and/or governing body
- › Undertaking annual risk assessments that consider and reflect the risks pupils face
- › Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 The ICT manager (Eduthing)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, including filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are protected from potentially harmful and inappropriate content and contact online, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses, malware and other cybersecurity risks, and that these protection systems are regularly updated
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous or inappropriate sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyberbullying are dealt with appropriately in line with the school's behaviour policy

- Reporting online safety-related issues or concerns to the online safety co-ordinator, DSL and/or headteacher as appropriate
- Managing the school's ICT systems to ensure that:
 - the school password policy is consistently applied and adhered to
 - systems are in place for misuse detection and protection against malicious attacks
 - access controls and encryption are used to protect personal and sensitive information stored on school-owned devices and systems
 - the school's web filtering systems are implemented, monitored and regularly updated
- Regularly monitoring the use of school technology, systems and online platforms, and reporting any actual or attempted misuse in accordance with school procedures
- Keeping up to date with relevant online safety guidance, cybersecurity developments and technical information in order to effectively carry out their role and support other staff where appropriate
- Ensuring appropriate backup procedures and disaster recovery plans are in place and regularly tested
- Maintaining accurate and up-to-date documentation relating to the school's network infrastructure, online security arrangements and technical procedures

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and implementing it consistently
- Reading, understanding, signing and adhering to the staff Acceptable Use Agreement/Policy (AUP), including any annual updates. New staff will sign the AUP as part of the induction process
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's acceptable use agreements (See Acceptable Use Policy)
- Maintaining an awareness of current online safety issues, legislation, guidance and good practice through training and continuing professional development (CPD)
- Modelling safe, responsible and professional behaviours in their own use of technology, both within and outside the school environment
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and understanding how to report concerns or incidents where filtering or monitoring systems may have failed by reporting it via our Child Protection Online Monitoring System/Management System (CPOMS)
- Following the correct procedures by requiring permission from the DSL or SLT if access to blocked or filtered content is required for legitimate educational purposes (usually emailed permission to Eduthing)
- Reporting any suspected misuse, safeguarding concern or online safety issue to the DSL, online safety co-ordinator or headteacher as appropriate

- Working with the DSL and safeguarding team to ensure that online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Making sure that incidents of cyberbullying are dealt with appropriately in accordance with the school's behaviour and anti-bullying policies
- Responding appropriately to all concerns relating to sexual violence and/or harassment, both online and offline, and maintaining an attitude of "it could happen here"
- Ensuring that school devices, systems and sensitive information are used and stored securely at all times

Exit Procedures

At the end of a period of employment, placement or volunteering, staff and volunteers must return any devices, equipment or resources loaned by the school. This includes providing PINs, passwords, access IDs or other relevant information required to allow devices and accounts to be securely reset, closed or transferred in accordance with school procedures.

3.6 Parents/carers

Parents and carers play a vital role in helping children to use technology safely, responsibly and positively. The school will work in partnership with parents and carers to promote safe and appropriate online behaviour both at home and at school.

Parents and carers are expected to:

- Read, understand and support the school's Pupil Acceptable Use Agreement and discuss its expectations with their child/children
- Ensure that their child has read, understood and agreed to the terms relating to the acceptable use of the school's ICT systems and internet
- Support the school in promoting safe, responsible and positive use of technology and the internet
- Encourage their child to develop safe online habits, including respectful online behaviour and the importance of reporting concerns
- Monitor and support their child's use of online platforms, games, apps and social media in an age-appropriate manner
- Understand that most social media platforms have a minimum age requirement of 13 years
- Reinforce key online safety messages at home, including the safe sharing of personal information, privacy settings and appropriate online conduct
- Encourage their child to speak to a trusted adult if they encounter upsetting, harmful or inappropriate online content or contact
- Consult with the school if they have concerns about their child's online behaviour, experiences, wellbeing or the use of technology by others within the school community
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Support the school's online safety and safeguarding procedures, including the appropriate use of devices and communication platforms
- Endorse and support the Parents'/Carers' Acceptable Use Agreement, where applicable

The school will provide parents and carers with online safety information, guidance and opportunities for engagement, including workshops, training sessions and signposting to appropriate resources, to help support children's safe use of technology at home.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- [UK Safer Internet Centre - What are the issues?](#)
- [Childnet - Help and advice for parents/carers](#)
- [Childnet - Parents and carers resource sheet](#)

3.7 Visitors and members of the community

Visitors, external agencies, contractors and members of the community who access the school's ICT systems, devices or internet services will be made aware of this policy and expected to read and follow it. Where appropriate, they will also be required to read, sign and adhere to the school's Acceptable Use Agreement before being granted access to school technology or online systems.

Visitors and members of the community are expected to:

- Support the school in promoting and maintaining a strong culture of online safety
- Use school technology and internet services safely, responsibly and professionally
- Model safe, respectful and positive behaviours in their own use of technology and online communication
- Report any online safety concerns, misuse or inappropriate behaviour to a member of school staff as soon as possible

3.8 Pupils

Pupils are responsible for:

- Reading, understanding, signing and adhering to the Pupil Acceptable Use Agreement
- Using the school's ICT systems, devices and internet access safely, responsibly and respectfully
- Understanding the importance of reporting online abuse, bullying, harmful content, misuse or access to inappropriate materials to a trusted adult
- Knowing what action to take if they, or someone they know, feels worried, unsafe or vulnerable when using online technology
- Understanding the importance of adopting safe, responsible and positive online behaviours both in and outside of school, and recognising that the school's online safety

expectations may also apply to conduct outside school where it affects the safety and wellbeing of members of the school community

- Respecting the privacy, rights and reputation of others online and refraining from behaviour that could cause harm or distress
- Contributing to pupil voice activities, surveys or discussions that help the school understand and improve pupils' online experiences and online safety provision
- Reporting any concerns relating to cyberbullying, harassment, exploitation, inappropriate contact or harmful online behaviour to a member of staff as soon as possible

4. Educating pupils about online safety

The statutory curriculum requires pupils to learn how to locate, retrieve, evaluate and exchange information using technology, including the internet. The school is committed to ensuring that all pupils are taught to use technology efficiently, safely, respectfully and responsibly, and to develop a mature and informed approach to accessing and interpreting online information.

Online safety is taught throughout the curriculum and embedded within Computing, Relationships Education, Health Education and other relevant subjects. Online Safety is taught explicitly through Project Evolve. In line with the school's safeguarding responsibilities, pupils are provided with as safe an online environment as possible through a combination of education, supervision, filtering and monitoring systems, and clear policies and procedures.

In accordance with the National Curriculum Computing Programmes of Study and the government's guidance on Relationships Education, Relationships and Sex Education (RSE) and Health Education, pupils will be taught age-appropriate online safety skills.

In Key Stage 1, pupils will 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

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour online
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people should be respectful in online interactions and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous

- The importance of avoiding pressure on others to share information or images online and strategies for resisting peer pressure
- How to critically evaluate online relationships and sources of information
- That people may behave differently online, including pretending to be someone else or pretending to be a child, and that this can lead to dangerous situations
- How to recognise harmful content or harmful contact and how to report concerns
- That there is a minimum age requirement for joining most social media platforms (currently 13 years old)
- The importance of protecting personal information online, including understanding privacy and location settings
- That material shared online may be copied, shared or circulated permanently and may not be fully removable
- That the internet contains content that may be inappropriate, upsetting or harmful and where to seek help and support if worried or concerned
- About the prevalence of deepfakes, including manipulated videos and images, and how these may be used to mislead people

The safe use of social media and the internet will also be reinforced across other curriculum areas where appropriate.

Where necessary, teaching about safeguarding, including online safety, will be adapted to meet the needs of vulnerable pupils, victims of abuse and pupils with SEND.

Practical Cyber Security Education

Pupils will also receive age-appropriate education about cyber security and safe use of technology, including:

- Password security and the importance of keeping passwords private
- Multi-factor authentication
- Methods used by hackers and criminals to trick people into sharing personal information, including phishing and social engineering
- The risks associated with removable storage devices such as USB drives
- How to report cyber incidents, attacks or concerns
- How to report a personal data breach

Pupils will also receive age-appropriate education about safeguarding risks online, including cyberbullying, online exploitation, inappropriate content and the risks of online radicalisation.

The school recognises that, despite careful filtering and monitoring systems, unsuitable material may occasionally be accessed online. Staff remain vigilant and any concerns regarding online content or access will be acted upon promptly, including blocking websites where necessary.

Any suspected personal data breach must be reported immediately to the Headteacher/DPO in accordance with the Data Protection Policy.

4.2 Filtering, Monitoring and Safe Use of Technology

The school uses a range of technical and organisational measures to help provide a safe online environment for pupils and staff. These include filtering and monitoring systems, secure network management, anti-virus and firewall protection, and appropriate access controls. The school uses SENSO, a cloud-based classroom management, safeguarding and IT monitoring system, to support the safe and appropriate use of technology across the school. SENSO enables authorised staff to monitor and support pupils' use of devices and online activity, identify potential safeguarding concerns, manage classroom device use and support the school's filtering and monitoring arrangements in line with safeguarding responsibilities.

Internet filtering is an essential part of the school's online safety provision. The school maintains up-to-date filtering, anti-virus and security systems designed to reduce the risk of exposure to inappropriate or harmful content and to protect users and devices from malicious software and unauthorised access.

The use of school equipment or networks to access, create, store or distribute inappropriate material is considered unauthorised use and will be addressed in accordance with the school's behaviour, safeguarding and disciplinary procedures.

To help protect the school network and users' data, pupils are not permitted to download executable files or install software without authorisation. Access permissions for staff and pupils are managed appropriately to reduce security risks.

The school acknowledges that no filtering system can guarantee complete protection from all online risks. Consequently, online safety education, active supervision and effective safeguarding procedures remain essential. Staff are expected to remain vigilant and report any concerns regarding online content, conduct or contact.

Requests to unblock websites for educational purposes should be made to the Computing Lead and the Headteacher, who will review the request and liaise with the school's filtering provider where appropriate.

The school will also work in partnership with parents and carers to promote safe and responsible use of technology at home. Training sessions, workshops, guidance and online safety information may be provided to support parents/carers in helping children stay safe online.

The school recognises that certain online behaviours may constitute criminal offences. These include, but are not limited to:

- The possession, creation or distribution of indecent images of children
- Online grooming or exploitation
- Unauthorised access to computer systems or data under the Computer Misuse Act 1990

- Sending malicious, threatening or harassing communications under relevant UK legislation

All online safety incidents and concerns will be managed in line with the school's safeguarding and child protection procedures.

5. Educating parents/carers about online safety

The school recognises the important role that parents and carers play in promoting online safety and supporting children to use technology safely, responsibly and positively.

The school will raise parents'/carers' awareness of online safety through regular communication, including letters, newsletters, the school website, workshops, training opportunities and other information shared with home. This Online Safety Policy will also be made available to parents/carers.

The school:

- Provides information for parents/carers which includes information about online safety at the point of entry through the Home School Agreement
- Runs a rolling programme of online safety advice, guidance and training for parents/carers
- Covers online safety during appropriate events
- Provides guidance and signposting to trusted online safety resources and organisations
- Allows parents/carers to communicate with teachers and school staff through approved school communication platforms, including comments on Google Classroom where appropriate

The school will inform parents/carers about:

- The systems used by the school to filter and monitor online activity
- What children are being asked to do online, including the websites, platforms and digital resources they may access through curriculum overviews e.g. Scratch

Any online interactions children may have with school staff as part of educational provision are through Google Classroom

Parents/carers are encouraged to work in partnership with the school to reinforce safe online behaviour and to support children in developing appropriate online habits both at home and at school.

If parents/carers have concerns or queries relating to online safety, these should be raised in the first instance with the Headteacher and/or the Designated Safeguarding Lead (DSL).

Concerns or queries regarding this policy may also be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying is bullying that takes place through digital technologies, including online platforms, social networking sites, messaging services, gaming platforms and mobile devices. Like all forms of bullying, cyber-bullying involves the repetitive and intentional harming of an individual or group by another individual or group, where there is an imbalance of power.

Cyber-bullying can include:

- Sending abusive, threatening or unkind messages
- Sharing images or personal information without consent
- Excluding individuals from online groups or activities
- Impersonating another person online
- Posting or forwarding harmful, offensive or humiliating content
- Encouraging others to participate in online bullying or harassment

Cyber-bullying will be treated with the same seriousness as any other form of bullying and will be managed in accordance with the school's Behaviour Policy and safeguarding procedures.

6.2 Preventing and Addressing Cyber-bullying

The school is committed to preventing cyber-bullying and promoting a culture of safe, respectful and responsible technology use.

Pupils will be taught about cyber-bullying through the curriculum, including Computing, PSHE, Relationships Education and other relevant areas of learning. Teaching will help pupils to:

- Understand what cyber-bullying is and the different forms it may take
- Recognise the impact cyber-bullying can have on individuals and the wider school community
- Understand how to respond safely and appropriately if they experience or witness cyber-bullying
- Know how and where to report concerns, including when they are a witness rather than the target of the behaviour
- Develop respectful and responsible online behaviour

Staff will actively discuss cyber-bullying with pupils and reinforce clear expectations regarding positive online conduct and digital communication.

All staff, governors and volunteers, where appropriate, will receive safeguarding and online safety training that includes awareness of cyber-bullying, its impact on children and appropriate responses and support strategies.

The school will also support parents and carers by providing information, advice and guidance about cyber-bullying, including recognising warning signs, reporting concerns and supporting children who may be affected.

Where incidents of cyber-bullying occur, the school will respond promptly and appropriately in line with the Behaviour Policy, Anti-Bullying Policy and safeguarding procedures. Support will be provided to pupils affected, and appropriate action will be taken to address the behaviour.

Where illegal, inappropriate or harmful material has been shared or distributed, the school will take all reasonable steps to contain the incident and minimise further harm.

The Designated Safeguarding Lead (DSL) will involve external agencies, including the police, where there are reasonable grounds to believe that a criminal offence may have been committed or where safeguarding concerns require additional support or intervention.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- › Poses a risk to staff or pupils, and/or
- › Is identified in the school rules as a banned item for which a search can be carried out, and/or
- › Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- › Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- › Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- › Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- › Cause harm, and/or
- › Undermine the safe environment of the school or disrupt teaching, and/or
- › Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the

police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- > They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- > The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- > **Not** view the image
- > Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- > The DfE's latest guidance on [searching, screening and confiscation](#)
- > UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- > Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

King Athelstan Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. King Athelstan Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

The school will develop guidance relating to the safe and appropriate use of artificial intelligence technologies.

Any use of artificial intelligence should be agreed with SLT (e.g. proofing reports/creating model texts) and must not include names of children or the school or photographs of the children or parts of the school that are easily identifiable. Staff must also check AI-generated content for accuracy, bias and suitability before using it with pupils.

7. Acceptable use of the internet in school

The school is committed to ensuring that all pupils are taught to use the internet and digital technologies safely, responsibly and effectively, and to develop a mature and informed approach to online behaviour and digital content.

In line with the school's safeguarding responsibilities, all reasonable and appropriate steps are taken to provide pupils, staff and the wider school community with a safe online environment. This includes a combination of education, technical safeguards, monitoring systems, filtering systems and clear policies and procedures.

All pupils, parents/carers, staff, volunteers and governors are expected to read and sign the relevant Acceptable Use Agreement regarding the use of the school's ICT systems and internet services. Visitors will also be expected to read and comply with the school's acceptable use expectations where appropriate.

Use of the school's internet, devices and ICT systems must be for educational purposes, professional responsibilities or other authorised school business only.

The school monitors the use of internet services, websites and online activity on school systems, where appropriate, to help ensure compliance with this policy, safeguarding responsibilities and acceptable use expectations. Access to online content is restricted through filtering and monitoring systems designed to reduce exposure to harmful, inappropriate or illegal material.

To reduce security risks and protect the integrity of the school network:

- Pupils are not permitted to download executable files or install unauthorised software
- Access permissions are managed appropriately for staff and pupils
- Users must not attempt to bypass filtering, monitoring or security systems
- Any concerns regarding online content or security must be reported immediately to a member of staff

The school recognises that no filtering or monitoring system can provide complete protection from all online risks and that inappropriate material may occasionally bypass these systems. Staff therefore remain vigilant and will take prompt action where concerns are identified, including requesting that websites are blocked where appropriate.

Requests to unblock websites for educational purposes should be directed to the Computing Lead or designated member of staff, who will liaise with the school's filtering provider where necessary.

Any misuse of the school's ICT systems or internet access will be addressed in accordance with the school's Behaviour Policy, Staff Code of Conduct, safeguarding procedures and disciplinary processes.

The school will continue to work in partnership with parents and carers by providing guidance, information and training opportunities to support safe and responsible internet use at home.

8 Managing Equipment and ICT Systems

The school is committed to ensuring that all ICT equipment, devices and systems are managed securely, responsibly and in accordance with safeguarding, data protection and health and safety requirements.

The school reserves the right to monitor internet use, email activity and the use of school ICT systems, and to examine, manage or delete files held on school equipment or networks where appropriate and in accordance with relevant legislation and school policies.

Network Security and User Access

To help ensure that the school network and ICT systems are used safely and securely, the school:

- Provides pupils from Year 1 onwards with individual usernames and passwords for accessing school systems where appropriate
- Requires all staff to keep usernames and passwords secure and confidential
- Makes clear that pupils must never use staff logins or passwords
- Ensures that access permissions are appropriate to users' roles and responsibilities
- Maintains separate areas and permissions for pupil and staff files and workspaces
- Requires users to log off or lock devices when unattended
- Requests that computers and devices are shut down appropriately at the end of the school day
- Restricts the downloading or installation of executable files and unauthorised software
- Reviews ICT systems and security arrangements regularly

The school also maintains appropriate filtering, monitoring, firewall and anti-virus systems to help prevent unauthorised access, malicious software and misuse of equipment or data.

Management of School Equipment

The school maintains equipment appropriately to support health and safety requirements and ensure systems remain secure and operational.

Remote access to the school network by external organisations or contractors will only be permitted where authorised and appropriately secured through approved providers or support services.

The school will ensure that personal or sensitive data transferred electronically is shared securely, encrypted where appropriate and managed in accordance with data protection legislation and Local Authority guidance.

Any breach of the school's acceptable use expectations or behaviour policies may result in disciplinary action in line with the Behaviour Policy. This may include confiscation of a device.

Confiscated devices will be stored securely and returned to parents/carers in accordance with school procedures.

8.1 Pupils using mobile devices in school

The school strongly discourages pupils from bringing mobile phones or personal smart devices into school unless there is a specific need agreed with parents/carers and the school, for example to support a child's safety when travelling to and from school independently.

Where pupils do bring mobile devices into school:

- Devices must be switched off or placed on silent mode and stored securely in accordance with school procedures
- Pupils are not permitted to use personal mobile devices during lessons, breaktimes, lunchtimes, clubs before or after school, or during any activities organised by the school unless specifically authorised by a member of staff for educational purposes
- Any use of personal devices must be in accordance with the school's Pupil Acceptable Use Agreement and Behaviour Policy

Pupils will be taught about the safe and responsible use of personal devices, including:

- Protecting personal information and phone numbers
- Communicating respectfully online
- Understanding appropriate boundaries for device use
- The risks associated with sharing images, videos or personal content online

Pupils are encouraged to share contact details only with trusted friends and family members and to report any concerns regarding online communication or device misuse to a trusted adult.

9. Staff using work devices outside school

Staff are expected to use school devices and personal devices responsibly, securely and professionally at all times, including when working remotely or outside of school.

Staff members must not use devices in any way that would breach the school's Acceptable Use Agreement, safeguarding procedures, confidentiality expectations or professional standards.

Use of Personal Devices

- Staff mobile phones, smart devices and personal cameras must not be used around pupils unless authorised for a specific school purpose
- Staff are not permitted to use personal mobile phones or devices to contact pupils, parents/carers or families in a professional capacity, either within or outside the school setting, unless authorised in exceptional circumstances
- Where communication with pupils or parents/carers is required, staff will use approved school communication systems or school-issued devices where available

- Mobile phones and personal devices should be switched off or set to silent mode during teaching time unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances
- Bluetooth and other sharing functions should be switched off or hidden when not in use to reduce security risks

In an emergency situation where a staff member does not have access to a school device, they may use a personal device to contact parents/carers or appropriate services. Where possible, staff should withhold their personal number by using 141 and must report the incident to the Headteacher or designated safeguarding lead as soon as possible.

Security of Devices

All staff members are responsible for taking appropriate steps to ensure that devices used for work purposes remain secure. This includes, but is not limited to:

- Keeping devices password protected using strong passwords or passphrases
- Ensuring devices automatically lock after a period of inactivity
- Keeping operating systems, software and applications up to date by installing security updates promptly
- Installing and maintaining appropriate anti-virus and anti-spyware software where applicable
- Ensuring that hard drives are encrypted to protect data if a device is lost or stolen
- Not sharing work devices with family members or friends
- Storing devices securely when not in use
- Taking reasonable precautions when accessing school systems remotely or using public networks

Work devices must be used primarily for professional purposes and in accordance with school policies and data protection requirements.

If staff have concerns about the security of a device or believe a device may have been lost, stolen or compromised, they must report this immediately to the Headteacher, Designated Safeguarding Lead (DSL), IT provider or other designated member of staff in line with the school's data protection and security procedures.

Failure to follow this policy may result in disciplinary action in accordance with the school's staff conduct and disciplinary procedures.

10. How the school will respond to issues of misuse

The school expects all members of the school community to use technology, devices, networks and internet services safely, responsibly and in accordance with this Online Safety Policy, the Acceptable Use Agreements, the Behaviour Policy, safeguarding procedures and the Staff Code of Conduct.

Whenever a pupil or staff member breaches the school's Online Safety Policy or acceptable use expectations, the final decision regarding sanctions or disciplinary action will be made by the Senior Leadership Team, taking into account the nature and seriousness of the incident and the relevant school policies and procedures.

Where appropriate, safeguarding procedures, the Child Protection and Safeguarding Policy, the Behaviour Policy and the Staff Code of Conduct will also be followed.

Responding to Inappropriate Online Content

If inappropriate or harmful online material is accessed within school:

1. Appropriate action will be taken to block or filter access to the material
2. The school's IT support provider and/or relevant technical support will be informed where necessary
3. The incident will be recorded and investigated as appropriate
4. Safeguarding procedures will be followed if there are concerns regarding a child's welfare or safety

Serious Misuse by Pupils

Serious misuse of school equipment, ICT systems or internet access by pupils may result in disciplinary action and, where appropriate, involvement of parents/carers, external agencies or the police.

Examples of serious misuse include:

- Repeated sending of messages or online communications that are considered bullying, harassing or threatening
- Deliberately accessing, downloading, creating or distributing material that is offensive, obscene, discriminatory, extremist, violent or pornographic
- Sharing or distributing content that breaches copyright, confidentiality or data protection legislation
- Attempting to gain unauthorised access to systems, accounts or data
- Deliberately damaging or disrupting school ICT systems or security
- Using technology in a way that brings the school into disrepute

- Recording, photographing or sharing images, audio or video without permission

Misuse by Staff

Where a staff member misuses the school's ICT systems or internet access, or misuses a personal device in a way that constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct, disciplinary procedures and safeguarding policies.

The action taken will depend on the individual circumstances and the nature and seriousness of the incident.

Advice and support may be sought from the Local Authority, LADO (Local Authority Designated Officer), HR providers or other relevant agencies where appropriate.

Where safeguarding concerns are identified, immediate action will be taken in accordance with safeguarding procedures, which may include suspension, referral to external agencies, and/or contacting the police.

The school will consider whether incidents involving illegal activity, harmful content or serious breaches of policy should be reported to the police or other appropriate authorities.

Anyone may report concerns about online abuse, exploitation or illegal online activity involving children to the Child Exploitation and Online Protection Command (CEOP) or the Internet Watch Foundation.

Further information and reporting tools are available from:

- [CEOP Safety Centre](#)
- [Internet Watch Foundation](#)

11. Training for staff, governors and volunteers

All new staff members will sign relevant agreements on arrival at the school e.g. Acceptable Use. They will receive training, as part of their induction through Level 2 Safeguarding training, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least every 2 years as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- › Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- › Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- › Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- › Develop better awareness to assist in spotting the signs and symptoms of online abuse
- › Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed annually by the Computing Lead, DSL and Senior Leadership Team. At every review, the policy will be shared with the governing body. From 2026-27 review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- › Child protection and safeguarding policy
- › Behaviour policy
- › Staff disciplinary procedures
- › Data protection policy and privacy notices
- › Complaints procedure
- › ICT and internet acceptable use policy
- › Anti-Bullying Policy
- › King Athelstan Cyber Incident Response Plan
- › Mobile Phone Policy
- › WhatsApp Groups Parents Code of Conduct
- › Anti-Radicalisation Policy
- › Whistleblowing Policy