

ASHCROFT INFANT AND NURSERY SCHOOL

Providing the best start in life for all children



Online Safety Policy

Headteacher: _____

Person Responsible for Policy and Review: Headteacher

Policy Type: Non - Statutory

DOCUMENT AND VERSION CONTROL

Version	Author	Implementation Date	Revision Detail
1.0	Jayne Fellows	September 2026	Completely rewritten to reflect current legislation

Contents

- 1 Aims
 - 2 Legislation and guidance
 - 3 Roles and responsibilities
 - 4 Educating pupils about online safety
 - 5 Educating parents and carers about online safety
 - 6 Cyber bullying and harmful online behaviour
 - 7 Acceptable use of the internet in school
 - 8 Pupils using mobile devices in school
 - 9 Staff using work devices outside school
 - 10 Responding to misuse
 - 11 Training for staff governors and volunteers
 - 12 Monitoring and review
 - 13 Links with other policies
- Appendix 1 EYFS and Key Stage 1 acceptable use agreement
- Appendix 2 Staff governors volunteers and visitors acceptable use agreement
- Appendix 3 Online safety training needs audit
- Appendix 4 Online safety incident log

1 Aims

This policy sets out how Ashcroft Infant and Nursery School keeps children and adults safe when using digital technology. Online safety is part of our whole-school safeguarding approach and is considered in the curriculum, staff training, filtering and monitoring, behaviour procedures and work with parents and carers.

Ashcroft Infant and Nursery School aims to:

- have robust processes to protect pupils, staff, volunteers and governors online
- identify and support pupils who may be at greater risk of online harm, including vulnerable pupils and pupils with special educational needs or disabilities
- educate the whole school community to use technology, including mobile and smart technology and artificial intelligence, safely and responsibly
- make sure concerns are identified, recorded, acted on and escalated promptly
- balance effective safeguarding controls with appropriate access to technology for teaching and learning.

The four categories of online risk

Category	What this includes
Content	Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm or suicide content, antisemitism, radicalisation, extremism, violence, misinformation, disinformation and conspiracy theories.
Contact	Harmful interaction with other users or applications that simulate human interaction, including peer pressure, commercial advertising, grooming and exploitation for sexual, criminal, financial or other purposes.
Conduct	Online behaviour that causes or increases the likelihood of harm, including bullying and making, sending or receiving explicit images, including images generated or altered using artificial intelligence.
Commerce	Risks including online gambling, inappropriate advertising, phishing, scams and other attempts to obtain money or personal information.

2 Legislation and guidance

This policy is based on the Department for Education statutory safeguarding guidance Keeping Children Safe in Education and relevant departmental advice and standards, including:

- Teaching online safety in schools
- Meeting digital and technology standards in schools and colleges
- Preventing and tackling bullying
- Relationships education and health education
- Searching, screening and confiscation
- Mobile phones in schools

- Protecting children from radicalisation and the Prevent duty.

It reflects relevant legislation, including the Education Act 1996, the Education and Inspections Act 2006, the Education Act 2011, the Equality Act 2010 and the Children's Wellbeing and Schools Act 2026. It also takes account of the National Curriculum computing programmes of study. As a maintained school, Ashcroft applies these requirements alongside Staffordshire local safeguarding arrangements and its own child protection procedures.

3 Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. It will make sure online safety remains an interrelated theme across safeguarding, curriculum planning, staff training, the role of the DSL and work with parents and carers.

The governing board will:

- make sure staff receive online safety training as part of safeguarding training and understand their filtering and monitoring responsibilities
- make sure pupils are taught how to keep themselves and others safe online
- make sure appropriate filtering and monitoring systems are in place on school devices and networks
- receive assurance that senior leaders review the effectiveness of filtering and monitoring at least annually
- consider the Department for Education filtering and monitoring standards with school leaders, the ICT lead and Wave 9
- monitor online safety incidents, risks and staff training needs through information provided by the DSL
- make sure teaching is adapted where necessary for vulnerable children, children who have experienced abuse and pupils with SEND.

All governors will read and understand this policy and agree to the staff, governor, volunteer and visitor acceptable use agreement in appendix 2. The safeguarding governor will provide oversight on behalf of the governing board.

3.2 The headteacher

The headteacher, Jayne Fellows, is responsible for making sure staff understand this policy and that it is implemented consistently. The headteacher will make sure there are effective cover arrangements when the DSL is unavailable so that safeguarding concerns are received, monitored and acted on without delay.

3.3 The designated safeguarding lead

The designated safeguarding lead is Jayne Fellows and the deputy designated safeguarding lead is Eluned Lane. Current safeguarding arrangements are also set out in the child protection and safeguarding policy and displayed in school.

The DSL has lead responsibility for online safety and will:

- support the headteacher to make sure this policy is understood and applied consistently
- review this policy annually with the headteacher and governing board
- understand the filtering and monitoring systems and processes used on school devices and networks
- provide governors with assurance that filtering and monitoring systems are effective and reviewed regularly
- work with the school ICT lead and Wave 9 to maintain appropriate technical systems and processes
- manage online safety concerns and incidents in line with the child protection and safeguarding policy
- respond to safeguarding concerns identified through filtering and monitoring
- make sure incidents, including cyber bullying, are recorded and dealt with appropriately
- provide staff training and updates, liaise with external agencies when necessary and report relevant themes to governors
- complete or oversee an annual online safety risk assessment which reflects the risks faced by Ashcroft pupils.

3.4 ICT support and Wave 9

The school's ICT lead, supported by Wave 9, is responsible for:

- maintaining appropriate security, filtering and monitoring on school devices and networks and reviewing these arrangements at least annually
- keeping systems secure and protected against viruses, malware and unauthorised access
- completing routine security checks and monitoring the school's ICT systems on a fortnightly basis
- blocking harmful or inappropriate content without unreasonably restricting teaching and learning
- preventing the downloading of potentially dangerous files where possible
- reporting filtering, monitoring and security concerns promptly to the DSL and headteacher
- supporting the investigation and secure recording of online safety incidents.

3.5 All staff and volunteers

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

- reading, understanding and consistently implementing this policy
- following the acceptable use agreement in appendix 2 and making sure pupils follow appendix 1
- knowing that the DSL leads on filtering and monitoring and reporting any failure or concern immediately to the DSL or deputy DSL
- not attempting to bypass filtering or monitoring; any access required for a legitimate educational purpose must be authorised by the headteacher or DSL and arranged through the ICT lead or Wave 9
- reporting and recording online safety concerns in accordance with the school's safeguarding procedures

- responding appropriately to concerns about online sexual abuse or harassment and maintaining an attitude that it could happen here
- protecting personal, safeguarding and school information when using digital systems or artificial intelligence tools.

3.6 Parents and carers

Parents and carers are expected to tell a member of staff or the headteacher about online safety concerns and to help their child understand and follow the acceptable use agreement in appendix 1. The school encourages families to use age restrictions, privacy controls and supervision appropriate to young children.

Further advice is available from the [UK Safer Internet Centre](#) and [Childnet](#).

3.7 Visitors and members of the community

Visitors and community users who access school ICT systems or the internet will be made aware of this policy and must follow it. Where relevant, they will be required to agree to the acceptable use terms in appendix 2.

4 Educating pupils about online safety

4.1 Curriculum and teaching

Online safety is taught in an age-appropriate way through the EYFS curriculum, computing, relationships and health education, PSHE, assemblies and other subjects when relevant. The school builds the foundations children need for later primary education while recognising the age and development of Nursery, Reception and Key Stage 1 pupils.

Pupils will be taught to:

- use technology safely, respectfully and responsibly
- keep personal information private and understand that passwords should not be shared
- recognise that people and information online may not always be who or what they appear to be
- understand that online actions can affect other people and that the same expectations of kindness apply online and face to face
- tell a trusted adult straight away if they see, hear or receive anything online that worries, upsets or confuses them
- understand in simple terms that images and words shared online can be copied and may be difficult to remove
- recognise that websites, games, social media and AI services have age limits and should only be used with appropriate adult permission and supervision
- know how to seek help and report concerns about content or contact.

Teaching will be adapted where necessary for vulnerable pupils, pupils who have experienced abuse and pupils with SEND. Staff will consider pupils' communication needs, understanding, experiences and the context in which technology is used at home and in school.

4.2 Practical cyber security

Pupils will receive simple, age-appropriate teaching about cyber security. This will include keeping usernames and passwords safe, protecting personal information, recognising suspicious messages or requests, looking after devices and reporting anything unusual to an adult. More technical concepts, such as phishing, social engineering, removable storage and multi-factor authentication, will be introduced only in ways that are meaningful and accessible for the age group.

5 Educating parents and carers about online safety

The school will raise awareness through its website, Class Dojo, letters, meetings and other communications. Information may include current risks, practical safety settings, age restrictions, cyber bullying, artificial intelligence and routes for reporting concerns.

Parents and carers will be told:

- that the school uses filtering and monitoring on its devices and networks
- what children are being asked to do online, including the websites or services they may access and whether they will interact online with anyone from school
- the school's expectations for any age-appropriate use of artificial intelligence
- who to contact if they have an online safety concern.

Queries or concerns should be raised with the class teacher, headteacher or DSL. Safeguarding concerns will be handled in accordance with the child protection and safeguarding policy.

6 Cyber bullying and harmful online behaviour

6.1 Definition

Cyber bullying is bullying that takes place online, including through messaging, social media, games or shared images. Like other bullying, it involves the repeated and intentional harming of a person or group where there is an imbalance of power. A single online incident may still be serious and will be addressed under the behaviour and safeguarding procedures even if it does not meet the definition of bullying.

6.2 Prevention and response

Children are taught in simple language what online bullying and unkind behaviour may look like, how it can affect others and how to get help. They are encouraged to tell an adult if something happens to them or if they witness it happening to someone else.

Class teachers address online behaviour through computing, PSHE and relationships education, supported by assemblies and targeted teaching where needed. Staff, governors and relevant volunteers receive safeguarding training on online abuse and cyber bullying. The school also shares information with parents and carers so that concerns can be identified and reported early.

The school will respond under its behaviour and safeguarding procedures. It will take reasonable steps to contain harmful material, support affected pupils, preserve evidence safely and involve external agencies where necessary. If the DSL has reasonable grounds to suspect that possessing material is illegal, the matter and relevant evidence will be referred to the police as soon as reasonably practicable.

6.3 Searching and examining electronic devices

The headteacher and staff specifically authorised by the headteacher may search for and confiscate an electronic device in line with the school's behaviour policy and the latest Department for Education guidance on searching, screening and confiscation. Any action will be reasonable, proportionate and informed by safeguarding considerations.

Authorised staff may examine and, only in exceptional circumstances, erase data or files where there is a good reason to do so. A good reason may exist where the device has been or could be used to cause harm, undermine the safe environment of the school, disrupt teaching or commit an offence.

If material may be evidence of an offence, it will not be deleted. The device will be secured and handed to the police as soon as reasonably practicable. If the material is not suspected evidence, deletion may be considered where its continued existence is likely to cause harm or where the pupil or parent or carer refuses to delete it.

If a member of staff suspects that a device contains a nude or semi-nude image of a child, including an image generated or altered using AI, they will not:

- view, copy, print, share, store, save or forward the image, or ask a child to share or download it
- delete the image or ask the pupil to delete it
- question pupils in detail about the imagery, as this is the responsibility of the DSL
- share information more widely than is necessary
- blame or shame any child involved.

The staff member will confiscate the device where lawful and safe to do so and report immediately to the DSL. If the image has already been viewed accidentally, this will also be reported immediately. The DSL will act in line with Department for Education and UK Council for Internet Safety guidance. Complaints about a search or deletion will be considered through the school complaints procedure.

6.4 Artificial intelligence

Ashcroft recognises that artificial intelligence can support teaching and learning but can also create safeguarding, accuracy, privacy and intellectual property risks. AI can be used to create convincing but false images, audio or video, including deepfakes and sexualised images, or to simulate relationships and give unsafe advice.

Pupils may use only school-approved, age-appropriate AI tools under direct adult supervision and for a clearly defined educational purpose. Staff will risk assess new AI tools or new uses of existing tools where they may affect pupils, staff or school information. Personal data, confidential information and safeguarding information must never be entered into a public or unapproved AI service. Any use of AI to bully, exploit, shame or impersonate another person will be treated seriously under the behaviour and safeguarding policies.

7 Acceptable use of the internet in school

Pupils and parents or carers will be asked to agree to appendix 1. Staff, governors, volunteers and relevant visitors will be asked to agree to appendix 2. School internet and ICT systems must be used for education or to carry out an authorised role. The school will monitor use and apply

filtering where appropriate. Monitoring will be lawful, proportionate and consistent with the school's data protection responsibilities.

8 Pupils using mobile devices in school

Ashcroft is a mobile phone-free school for pupils. As an infant and nursery school, pupils are not expected to bring mobile phones or smart devices with similar functionality, including smart watches, into school. Pupils must not have access to or use such devices at any point during the school day, including lessons, playtimes, lunchtimes, clubs and wraparound provision.

An exception may be agreed only by the headteacher for a documented medical, safeguarding or other significant individual need. Any permitted device must be used strictly in accordance with the agreed arrangement.

If a pupil brings a device without an agreed exception, it must remain switched off and will be handed to the school office or a member of staff for safe keeping. It will be returned to the parent or carer. Misuse may lead to a proportionate response under the behaviour policy.

9 Staff using work devices outside school

Staff must take appropriate steps to keep work devices and school information secure. They must:

- use a strong password and never share it
- keep the device and hard drive encrypted where this is provided or required
- make sure the device locks automatically when left inactive
- not allow family members or friends to use the device
- keep anti-virus, anti-spyware, operating systems and applications up to date
- use only authorised software, services and storage
- use encrypted removable storage where the school has authorised its use
- keep the device physically secure and report any loss, theft, suspected breach or security concern immediately to the headteacher, DSL and ICT lead
- use work devices only for authorised work activities and in accordance with appendix 2 and the data protection policy.

Staff must not use personal devices to take or store photographs, videos or recordings of pupils unless this has been expressly authorised under an agreed school procedure. School data must not be transferred to personal accounts or unapproved services.

10 Responding to misuse

Where a pupil misuses school ICT or the internet, the school will follow its behaviour, safeguarding and acceptable use procedures. The response will reflect the child's age and understanding and the nature, context and seriousness of the incident. Support, education and restoration will be considered alongside any sanction.

Where a staff member misuses school ICT, the internet or a personal device in a way that may constitute misconduct, the matter will be managed under the staff code of conduct and disciplinary procedures. The school will consider referral to the local authority, safeguarding partners, the Local Authority Designated Officer, the police or other agencies where appropriate.

11 Training for staff governors and volunteers

New staff will receive online safety training during induction. All staff will receive refresher training at least annually as part of safeguarding training, together with updates when risks, technology or guidance change. Governors will receive online safety training within their safeguarding training and volunteers will receive training appropriate to their role.

Training will make clear that technology is a significant component of many safeguarding and wellbeing concerns and that children can abuse other children online. This can include:

- abusive, threatening, harassing or misogynistic messages
- non-consensual sharing of nude or semi-nude images or videos, including AI-generated or altered images
- sharing abusive images or pornography with someone who does not wish to receive it
- online elements of physical abuse, sexual violence, coercion or initiation behaviour.

Training will help staff recognise signs of online abuse, respond to disclosures, understand filtering and monitoring responsibilities and help pupils recognise risks and make safer choices. The DSL and deputy DSL will complete safeguarding training, including online safety, at least every two years and update their knowledge at least annually.

12 Monitoring and review

The DSL will make sure behaviour and safeguarding concerns relating to online safety are recorded. Appendix 4 provides a paper incident log where required, but safeguarding concerns must also be recorded through the school's normal safeguarding recording process.

The headteacher and DSL will review this policy annually and sooner where legislation, statutory guidance, technology, risk or school practice changes. The governing board will approve each review. The review will be informed by an annual online safety risk assessment, filtering and monitoring checks, incident patterns, curriculum review and training needs.

13 Links with other policies

This policy should be read alongside the school's:

- child protection and safeguarding policy
- behaviour policy and anti-bullying procedures
- staff code of conduct and disciplinary procedures
- data protection policy and privacy notices
- complaints procedure
- relationships and health education and curriculum policies
- any current ICT security, artificial intelligence, mobile technology or acceptable use procedures.

Appendix 1 EYFS and Key Stage 1 acceptable use agreement

This agreement uses simple rules for the children at Ashcroft Infant and Nursery School. Adults will explain the rules in language appropriate to each child's age and needs.

When I use school computers, tablets or the internet, I will:

- ask a teacher or adult before I use them
- use only the websites, apps and AI tools that a teacher or adult has allowed me to use
- use them only in the way the adult has explained
- use kind words and treat other people respectfully
- keep my name, address, telephone number and other personal information private unless a trusted adult says it is safe to share
- keep my username and password private
- look after school equipment and tell an adult if something is broken or not working
- tell an adult straight away if I click something by mistake, receive a message from someone I do not know or see anything that worries or upsets me
- use school devices for schoolwork only
- log off or close the device when I have finished.

I understand that the school checks how its devices and internet are used and that an adult will help me if I make a mistake or do not follow the rules.

Parent or carer agreement I agree that my child may use the school's ICT systems and internet when appropriately supervised. I will help my child understand and follow these rules and will raise any concerns with the school.

Appendix 2 Staff governors volunteers and visitors acceptable

When using school ICT systems or the internet, including outside school on a work device where applicable, I will not:

- access, create, link to, send or share inappropriate, violent, criminal, abusive or pornographic material
- use systems in a way that could harm a child, another person or the school's reputation
- access social networking sites or chat services for personal use through school systems
- use improper, discriminatory or offensive language in online communication
- install unauthorised software or connect unauthorised hardware or devices
- enter personal pupil data, confidential information, safeguarding information or sensitive school data into a public or unapproved AI tool
- share passwords or use another person's account
- take photographs or recordings of pupils without authorisation and a clear school purpose
- share confidential information or access, alter or disclose data without authority
- promote a private business unless it is directly related to authorised school activity.

I will:

- use school systems only for education or the authorised duties of my role
- follow school procedures for data protection, safeguarding, AI use, mobile technology and information security
- take reasonable steps to keep devices secure and password protected
- report any pupil concern, harmful material, filtering or monitoring failure, lost device or suspected data breach immediately through the correct school procedure
- use AI only for an authorised purpose and check outputs carefully for accuracy, bias, safety, confidentiality and suitability
- use school ICT responsibly and make sure pupils in my care do the same
- accept that the school may lawfully and proportionately monitor the use of its systems and facilities.

Appendix 3 Online safety training needs audit

Online safety training needs audit		
Question	Yes	No Comments
Do you know who has lead responsibility for online safety?		
Do you know how to report an online safety or safeguarding concern?		
Are you aware of ways children can abuse other children online?		
Do you understand the procedure for suspected nude or semi-nude images?		
Are you familiar with the relevant acceptable use agreements?		
Are you familiar with filtering and monitoring on school devices and networks?		
Do you understand your responsibilities if filtering or monitoring fails?		
Do you know the process for requesting legitimate access to blocked content?		
Do you use strong, unique passwords and follow the school's account security requirements?		
Do you understand the privacy and safeguarding risks of generative AI?		
Are you familiar with the school's response to cyber bullying?		
Is there any area in which you need further training? Please give details.		

Appendix 4 Online safety incident log

Use this log where a paper record is required. Safeguarding concerns must also be recorded and escalated through the school's normal safeguarding procedures.

[illegible]