Ashton West End Primary Academy
Online Safety Policy

Approved by: The full governing body Date: 15th March 2023

Last reviewed on: 18th January 2023

Next review due by: February 2024

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department'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 board

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

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

The governor who oversees online safety is Mrs Eleanor Beswick.

All governors will:

- Ensure that 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 (appendix 3)

3.2 The Principal

The Principal is responsible for ensuring that all staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and DDSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- Ensuring that the staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the ICT manager and other staff, as necessary, to facilitate technical solutions in relation to filtering and monitoring and security of the network and devices.
- Ensuring that any online safety incidents are logged in our CPOMS system and dealt with appropriately in line with the school behaviour, safeguarding and online policies.
- Ensuring that any incidents of cyber-bullying are logged in our CPOMS system and dealt with appropriately in line with the school behaviour, safeguarding and online policies.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs) Sharing information, advice and guidance around online safety on a regular basis via newsletters, bulletins.

- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing board and members of staff.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged in our CPOMS system and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour, safeguarding and online policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour, safeguarding and online safety policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3). Visitors will be told how to escalate incidents if they encounter something in school.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. We will explore the key areas from the

Education for a Connected World Framework.

They are:

Self image and identity
Online Relationships
Online Reputation
Online Bullying
Managing Online Information
Health Wellbeing and lifestyle
Privacy and Security
Copyright and Ownership

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will be available for parents to view on our website.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also has a section on the school website to support pupils and parents if they need help or advice with who to report to.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices (Filtering and Monitoring)

All of the school devices are filtered and monitored with daily and weekly alerts and reports sent to the DSL. Filtering and monitored is reviewed annually to check for effectiveness.

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:

- Make an assessment of 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 or an appropriate staff member

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

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 if 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 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 / searches and confiscation 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will filter the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. Furthermore, we will monitor further activity on devices to ensure our whole school community are effectively safeguarded.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident and escalated in line with our polices and procedures.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training

All new staff members will receive training, as part of their induction, 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 once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and DDSL 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. They will receive annual training as well as regular updates.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy. Further information, advice and guidance in relation to digital safeguarding, trends and themes will be disseminated within the safeguarding team throughout the academic year.

10. Monitoring arrangements

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

This policy will be reviewed every year by the DSL/Principal. At every review, the policy will be shared with the governing board.

11. Keeping children safe whilst accessing learning from home

Remote learning, also often referred to as distance learning, is simply a method of learning which doesn't require face-to-face contact with the teacher in a physical location. It means children can learn away from the classroom and often employs online methods such as webinars, e-learning, live-streaming or the

ability to download resources and materials. At Ashton West End Primary Academy, we have ensured that there are a range of ways that our children can access learning from home.

At AWEPA, we use ClassDojo. ClassDojo is a school communication platform that teachers, students, and families use every day to build close-knit communities by sharing what's being learned at home through photos, videos, and messages. ClassDojo has been certified by iKeepSafe, an FTC-approved COPPA Safe Harbor, for compliance with their COPPA Safe Harbor program. ClassDojo does not ask for, or require, children to provide personal information beyond that which is reasonably necessary to use ClassDojo. Information collected from students is never used or disclosed for third-party advertising or any kind of behaviorally-targeted advertising, and it is never sold or rented to anyone, including marketers or advertisers. To ensure that only children from AWEPA can access their ClassDojo account, the children have their own private QR code which allows them to log into their class page. The children keep the QR code private and do not share it with anyone else.

As a school, we also use Google Classroom to facilitate online learning for our children. Google Classroom can be used as a secure place to store, organize, share, and access information from any device. All you need is a web browser, such as Microsoft Edge, Internet Explorer, Chrome, or Firefox. To ensure that the children are kept safe whilst using Google Classroom they have a private username and password.

To ensure that our children stay safe whilst accessing online learning from the platforms above, we have:

- Ensured that our pupils do not need to sign up to anything with a personal email address. Children are provided with a school email address or a username and password.
- Taken the time to continually educate our children on the importance of online safety. We ensure that our pupils understand that they need to always keep their login to all facilities private and that they do not share their account with anyone.
- Discussed as a staff team how important it is to monitor our online learning platforms. Staff monitor all platforms where children can interact (Google Classroom and Class Dojo). All teachers monitor this, as well as the Computing lead and members of SLT. It is important for us to monitor the use of these facilities and for us to ensure that every child understands what is appropriate to write online. At school, we constantly remind children that these messages will be visible to the school staff and they should not put anything in a message, that they would not want anyone else to see.
- Chosen online platforms where there is no unnecessary personal information in the user profile of these apps. For example: Children's location, phone number and dates of birth are kept private.
- Kept all online platforms up-to-date with careful monitoring. Our Computing Lead and ICT Technician ensures that there are no security flaws in these applications. They make sure that all of our online learning platforms are kept up-to-date.

In a school closure situation, pupils working at home will receive a weekly phone call from a member of staff and where there are concerns, there will be a house visit and the correct agencies will be contacted and protocols followed. Vulnerable pupils will be monitored by the school SENCO and encouraged to attend school.

Google Classroom Meet – A Teacher's Guide for Safety

Before the meeting:

- Teachers to provide children with the instructions of how they can attend the meeting. E.g., date, time and how to attend. Give children advance warning of this and post reminders. You can send this information via email to the office staff, and they can send out information via Parent Mail to try to increase numbers of attendees.
- Before the meet, write down the rules for the children to follow during the meeting. E.g.

*Hi year *! I am very excited to meet with you all tomorrow at 2pm. Please make sure that you have your video on and your microphone off when you first attend the meeting. If your video is off, I will have to remove you from the meeting. I look forward to seeing you then!*

- Ensure that you know how to end the meeting in case of an emergency.
- Learn how to mute and unmute all participants. This way, if a child is saying something inappropriate, all microphones can be quickly switched off.
- Ensure that you know how to remove children from the meeting.
- Be conscious of background environments and others in the room. Ensure that what the children can see behind you is child friendly.
- Arrange for a member of staff to join you on the Google Meet. This will ensure that you are never alone with a child. **There should always be two members of staff present.**
- 1:1 video conferencing is strictly prohibited – on no occasion should staff make or take 1:1 video calls with pupils.
- Please ensure that members of staff are dressed appropriately (when working from home) and that children are asked to do so prior to the meeting too.
- If class teacher is isolating, partner teacher to hold their Google Meet for them in school.

At the start of the meeting:

- At the start of each meeting, please tell / remind children about the Google Meet rules:
    - Videos on at all times. If children switch their video off, they will be removed from the Google Meet and parents will be contacted
    - Showing respectful behaviours to others at all times
    - Dressed appropriately
    - Ensure that they are in a position so that their background is appropriate
- It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate, referrals should still be made to safeguarding leads.
- When using Google Meet, two staff should be present on all calls at all times. ·
- Staff will remove any participants who are not following all of the guidelines and parents to be contacted.
- The meeting will be ended if the member of staff witnesses or hears anything of concern. The details will be passed to the DSL.
- **Government guidance is that Google Meets are not recorded.**

After the meeting:

- Teachers are to reset the google meet link. This will mean that children cannot access the meet once the teacher has left.

12. 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

Ashton West End Primary Academy

EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Ashton West End Primary Academy

KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission • I will hand my mobile phone in at the main office at the start of the day and collect it again at the end of the day. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	