Ashleigh Primary School and Nursery, Wymondham

"We are all stars. Ashleigh helps us shine."

Online Safety Policy

Persons Responsible –
Online Safety Lead, Senior Leadership Team, Governors

Date of Policy: January 2024 **Next Review Due: September 2024**

Adopted by Full Governing Body

Signed ..... **Date .....**

Contents

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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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
- Relationships and sex 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 board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher 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 Jonathan Brophy.

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)

The governing board must ensure 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 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 their safeguarding needs.

3.2 The Headteacher

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

The Headteacher will receive daily alerts of online incidents in school including internet filtering updates. The Headteacher holds strategic responsibility for ensuring the school meets the standards for filtering and monitoring.

3.3 The designated Online Safety Lead and other Designated Safeguarding Leads

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

The DSL named as Online Safety Lead (Hannah Meek) takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT technician 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 Safeguarding policy
- Ensuring that any online safety incidents or cyberbullying incidents are logged and dealt with appropriately in line with this policy and the school's 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 board
- Working with the Headteacher to ensure that the school continues to meet the standards for filtering and monitoring https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

3.4 The ICT Technician

The ICT technician is responsible for:

- Following strategic direction from the Headteacher around filtering and monitoring
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 monthly full security checks, monitoring the school's ICT systems and reporting to the Headteacher.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported to the Headteacher.

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 on CPOMS and dealt with appropriately in line with this policy
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking to the Headteacher or DSL.

- Discussing with the Headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Ensuring that any incidents of cyber-bullying are reported on CPOMS so that they can be dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher 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 (Appendix 1)

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).

4. Educating pupils about online safety

Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online Safety is embedded into our PSHE and Computing curricula through real life scenarios and questions (See Appendix 5). At Ashleigh, the long term plan for the teaching of Online Safety through PSHE and Computing has been informed by:

- DfE Teaching Online Safety in Schools
- SWGfL Project Evolve – online safety curriculum programme and resources

Each year children will cover the following topics in an age-appropriate way:

-Self-image and Identity

-Online Reputation

-Online bullying

-Managing Online information

-Health, Wellbeing and Lifestyle

-Privacy and Security

-Copyright and Ownership

As well as the planned online safety curriculum, key online safety messages will be reinforced in assemblies and in all lessons where technology is used. Children will consistently be taught about the 'Safeguarding hand' to identify 5 safe adults who they could talk to if they were worried about online safety.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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 or learning platforms. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings if appropriate or in response to a reported incident.

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

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

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.

Cyberbullying will be a key element covered in our PSHE curriculum (See appendix 5).

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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 monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school if they have a reasonable reason to do so (e.g. walking to and from school alone), but they are not permitted to use them during the school day or on the school site. They should hand in their phones to the class teacher on arrival and ask for them back at the end of the school day.

Children should not bring smart watches to school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) All access to the school email and OneDrive will require multi-factor identification.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring that anti-virus and anti-spyware software is up to date and informing ICT technician of the need for any updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

10. 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 policies on behaviour and acceptable use 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, the risks of online radicalisation and how the school's filtering and monitoring system works.

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).

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, 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 the risks up
- 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 and deputies 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

Logs of all behaviour and safeguarding issues related to online safety should be uploaded to CPOMS.

This policy will be reviewed every year by the Online Safety Lead (DSL). At every review, the policy will be shared with the governing board. 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
- Curriculum for Life Policy
- Guidance for safer working practice for those working with children and young people in education settings code of Practice (May2019)

Appendix 1: Acceptable Use agreement for pupils/ parents and 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:
 	
• Always ask a teacher before using computers or iPads.
• Only use websites that a teacher or adult has allowed me to use
• Tell my teacher straight away if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that upsets or worries me.
• Only use the computers and iPads for my learning.
• 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.
• Never share my username or 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
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
• I will always get permission from others before taking a photo or video.
• I will not download anything or click on links in emails without permission from an adult.
If I need to bring a personal mobile phone or other personal electronic device into school for safety reasons:
• I will give this to my teacher to be locked in a cupboard during the day. I will then ask for it back at the end of the day.
• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
• I will not take photos or videos at school using my personal device.
 	
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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Ashleigh Primary School and Nursery, Wymondham, Norfolk

Acceptable Internet Use Agreement

The computer system is co-owned by the school and is made available to the children to further their education and to staff to enhance their professional activities including teaching, research administration and management. This school's Internet Access Policy has been drawn up to protect all parties - the children, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff requesting Internet access should sign up a copy of this acceptable Internet Use Statement and return it to the Online Safety Lead.

- All internet activity should be appropriate to staff professional activity or the children's education;
- Access should only be made by the authorised staff/adults and supervised pupils, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all email sent and for contacts made that may result in any email being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- All staff must adhere to the Principles of 'Guidance for Safer Working Practices'
- All staff must be aware of the filtering and monitoring systems in place and report any concerns that the system may be compromised immediately to the Headteacher or DSL.
- Use of the network (including through personal devices) for any activity that would be inappropriate in a school setting, including accessing pornographic, racist or offensive material is forbidden. On the rare occasions that inappropriate sites are accessed i.e. not screened by the school's filtering and monitoring, they should be reported to the Headteacher;
- No access to chat rooms;
- All computer access is subject to Headteacher approval.
- Any illegal, inappropriate or harmful material or incident, should be reported to the Online Safety Lead or a Designated Safeguarding Lead.
- Images of others should only be taken or published with their permission. Personal equipment should not be used to record these images.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Full name _____ Post _____

Signed_____ Date _____

Appendix 3: 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?	
Are you aware of the ways pupils can abuse their peers online?	
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?	

Appendix 4- Ashleigh PSHE Curriculum Online Safety Progression

National Curriculum expectations:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

	Online Safety Questions/debate topics covered in PSHE **(Copyright, Privacy and Security will be covered in more depth in Computing lessons)**
Reception	What does online mean? What does it mean to share something online? How can people talk to each other using the internet? How do we keep safe online? What rules can help me stay safe and healthy when using technology?
Year 1	Who can help me if I feel upset about something I see online? Why do I need to ask before using the internet? What is personal information? How can I choose kindness online? How might I react if I lose a computer game? Is money spent online real money?

Year 2	What is the internet and how do I stay safe online? Should I play on an x-box all day? What should I do if I see something that worries me on YouTube? Can bullying happen online? What should I share online? People sometimes use the internet or digital devices in their work.
Year 3	Would you say that to my face? What is online bullying? Who is in my online community? Is it OK to change your mind about someone online? How can the internet help us? What is personal information? What is an online identity? Why do some things have age restrictions?
Year 4	Is it healthy to follow the rich and famous on social media? Am I proud of how I act online? Everyone was saying it so I just hit the 'like' button. Should children be allowed to access online banking? Do you know who you are talking to online? Are mobile phones ruining family meal times? Once it's out there, it's out there forever.
Year 5	What does online safety mean? How can my online behaviour impact others? Who's watching me online? I googled it so it must be true. How does the internet influence me? How can the internet influence consumer food habits?
Year 6	What are the pros and cons of the online world? Am I in control when online? I said it online so it's okay. It's not real. Who am I influenced by online? My online self and my real self. Two separate people? Are age restrictions online taken seriously? Why bother? How do I stand up to online bullying? How does social media impact mental health? Online comments: cowardly or brave? How does the internet help gangs to function? Should social media be used as a portal to vent negative emotions?