Ashford Oaks Primary School

Oak Tree Road, Ashford, TN23 4QR

Online Safety Policy
January 2025

Document history: Reviewed by Sarah-Jane Sullivan & Jane Marshall Reviewed by Jane Marshall Reviewed by Jane Marshall Reviewed by Jane Marshall Reviewed by Jane Marshall Reviewed by Jane Marshall Reviewed by Jane Marshall Reviewed by Jane Marshall	May 2018 Sept 2019 Jan 2020 Jan 2021 Jan 2022 Jan 2023 Jan 2024 Jan 2025
Safeguarding Reviewed by Theresa Dickins	13 January 2025
Agreed by the governing body on:	15 January 2025
Review date: Annually	**January 2026**
Signed: Rob Cooke **Chair of Governors**	

Key Details

Designated Safeguarding Lead: Jane Marshall

Named Governor with lead responsibility: Toni Harris

This policy will be reviewed <u>at least</u> annually. It will also be revised following any concerns

Contents:

Ashford Oaks Primary School
Online Safety Policy

1. Policy Aims

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, <u>Keeping Children Safe in Education</u>, and its advice for schools, the UN Convention on the Rights of the Child on:

- o Teaching online safety in schools
- o Preventing and tackling bullying, sexual harassment/bullying, child exploitation and cyber-bullying: advice for headteachers and school staff
- o Relationships and sex education
- o Safeguarding Children Multi-agency Partnership (KSCMP) procedures
- o As a Rights Respecting school, Articles 3, 8, 12, 17 and 19 refer.

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 purpose of Ashford Oaks Community Primary School online safety policy is to:

- o Safeguard and promote the welfare of all members of Ashford Oaks Primary School community online.
- o Identify approaches to educate and raise awareness of online safety throughout our community.
- o Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- o Identify clear procedures to use when responding to online safety concerns.

Ashford Oaks Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- o **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- o **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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

o **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

o **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Policy Scope

o Ashford Oaks Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

o Ashford Oaks Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.

o Ashford Oaks Primary School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to risk.

o This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as learners and parents/carers.

o This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with school issued devices for use on off-site.

Links with other policies and practices

This policy links with several other policies, practices and action plans including but not limited to:

o Behaviour and Anti-bullying policy
o Acceptable Use Policies (AUP) and/or the Code of conduct
o Child Protection policy
o Induction policy
o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
o Data Protection policy
o Safeguarding and Child Protection

3. Monitoring and Review

Technology evolves and changes rapidly as such Ashford Oaks Primary School will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local child protection concerns or any changes to the technical infrastructure.

- o We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- o To ensure they have oversight of online safety, the headteacher/DSL will be informed of online safety concerns, as appropriate.
- o The named Governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the Governing Body.
- o Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- o **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 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 Toni Harris

All governors will:

- o Ensure that they have read and understand this policy

- o Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

- o Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

- o Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

- o **The Headteacher**

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

o **The Designated Safeguarding Lead (DSL**).

The DSL [and deputies] are set out in our child protection policy as well as relevant job descriptions.

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

- o Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- o Working with the headteacher, ICT network manager and other staff, as necessary, to address any online safety issues or incidents

- o Managing all online safety issues and incidents in line with the school child protection policy

- o Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- o Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- o Updating and delivering staff training on online safety

- o Liaising with other agencies and/or external services if necessary

- o Providing regular reports on online safety in school to the headteacher and/or governing board

- o Review filtering and monitoring provision at least annually.

- o 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

This list is not intended to be exhaustive.

o **The ICT Network Manager**

The ICT network manager is responsible for:

- o Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- o Conducting a full security check and monitoring the school's ICT systems on a 2/3 times weekly basis and discuss with DSL.

- o Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- o Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- o Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour and anti bullying policy

This list is not intended to be exhaustive.

All staff and volunteers

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

- o Maintaining an understanding of this policy
- o Implementing this policy consistently
- o 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 terms on acceptable use
- o Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- o Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour and anti bullying policy
- o 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'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- o Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- o Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

- o What are the issues? – UK Safer Internet Centre
- o Hot topics – Childnet International
- o Parent resource sheet – Childnet International

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.

5.   Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- o Relationships education and health education in primary schools
- o To help minimise concerns Ashford Oaks will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and harassment by implanting a range of age and ability appropriate educational methods as part of our curriculum (**NSPCC Speak**

out, stay safe, Workshops in Year 5 and 6, NSPCC Share Aware and Pantosaurus, Digiducks Big Day Story, Internet Safety Day and Social Media Ambassadors).

In **Early Years** and **Key Stage 1**, pupils will be taught to:

- o Use technology safely and respectfully, keeping personal information private

- o 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:

- o Use technology safely, respectfully and responsibly

- o Recognise acceptable and unacceptable behaviour

- o Identify a range of ways to report concerns about content and contact

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

- o That people sometimes behave differently online, including by pretending to be someone they are not

- o 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

- o The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- o How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- o How information and data is shared and used online

- o What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- o How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

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

6.   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 our termly parent workshop, This policy will also be shared with parents.

The school will let parents know:

- o What systems the school uses to filter and monitor online use

- o What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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.

7. Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also Ashford Oaks behaviour and anti bullying policy.)

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.

Ashford Oaks 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 pupils.

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 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 Ashford Oaks behaviour and anti bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, Ashford Oaks will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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:

- o Poses a risk to staff or pupils, and/or

- o Is identified in the school rules as a banned item for which a search can be carried out, and/or

- o 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:

- o 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 / DSL]

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

- o 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:

- o Cause harm, and/or

- o 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 staff member in conjunction with the DSL / 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:

- o They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

- o 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:

- o **Not** view the image

o 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 <u>screening, searching and confiscation</u> and the UK Council for Internet Safety (UKCIS) guidance on <u>sharing nudes and semi-nudes: advice for education settings working with children and young people</u>

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

o The DfE's latest guidance on <u>searching, screening and confiscation</u>

o UKCIS guidance on <u>sharing nudes and semi-nudes: advice for education settings working with children and young people</u>

o Ashford Oaks behaviour and anti bullying policy

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

8. 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. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the Ashford Oaks 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.

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:

o 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)

o 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

o Making sure the device locks if left inactive for a period of time

o Not sharing the device among family or friends

o Installing anti-virus and anti-spyware software

o Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate Ashford Oaks's terms of acceptable use.

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 network manager].

Officially provided mobile phones and devices
- CSLT will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- CSLT mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- CSLT mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies
- School phones will be easily identifiable as they will be in a orange case.

10.   How the school will respond to issues of misuse
Concerns about pupils online behaviour and/or welfare
- The DSL or deputy will be informed if online safety incidents involve safeguarding or child protection
- The DSL or deputy will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures
- The school will inform parents of any incidents or concerns involving their child, as and when required
- Ashford Oaks recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers, all abuse will be responded to in line with our child protection and behaviour and anti bullying policies.

Concerns about staff online behaviour and/or welfare
- Any complaint about staff misuse will be referred to the Headteacher or DSL, according to the our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.
- Welfare support will be offered to staff as appropriate

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 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).

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

- o Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- o Children can abuse their peers online through:

  - o Abusive, harassing, and misogynistic messages

  - o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

  - o Sharing of abusive images and pornography, to those who don't want to receive such content

  - o 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 [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.

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

Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Online Safety
  - Tel: 03000 415797
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
  - Kent e–Safety Blog: www.kentesafety.wordpress.com

KSCMB:

- www.kscmb@kent.gov.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours: 03000 41 91 91
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- UK Council for Internet Safety (UKCIS): www.gov/government/organisation/uk-council-for-internet-safety
- Parent Zone https://parentzone.org.uk
- Parent Info https://parentinfo.org
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com

- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk