ANGLIAN LEARNING

Dynamic, empowered learners who thrive and lead in their communities: locally, nationally and globally

ONLINE SAFETY POLICY

THIS POLICY WAS APPROVED:	SUMMER 2026
POLICY VERSION:	3.0
THIS POLICY WILL BE REVIEWED:	AUTUMN 2027
MEMBER OF STAFF WITH RESPONSIBILITY FOR REVIEW:	DIRECTOR OF INCLUSION
THIS POLICY WAS CONSULTED WITH:	DESIGNATED SAFEGUARDING LEAD, DIRECTOR OF PEOPLE AND DIRECTOR OF ICT
THIS POLICY WAS DISTRIBUTED TO:	CONNECT

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Online safety is treated as a safeguarding matter and is embedded as a running and interrelated theme throughout the Trust's safeguarding culture, policies, curriculum, staff training and governance oversight. It is not a standalone strand but integral to our whole-school safeguarding approach.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2025 (KCSIE), 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
- Sharing nudes and semi- nudes: advice for education settings (UKCIS December 2020)
- Revised Prevent Duty guidance (April 2021)

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.

KCSIE categorises the breadth of online safety issues into four areas of risk, the four 'C's:

- CONTENT:
  being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- CONTACT:
  being subjected to harmful online interaction with other users; for example: 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; for example, 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 scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Stapleford Community Primary School recognises that online risks evolve rapidly, including those associated with generative artificial intelligence (AI), AI-generated intimate images (including deepfakes), sextortion, financial exploitation, misinformation and disinformation. These risks are addressed through safeguarding systems, curriculum design and governance oversight.

The School will deal with online safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, such as *the Child Protection and Safeguarding Policy and Positive Behaviour and Relationships policy.* It will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

3. Roles and Responsibilities

3.1. Anglian Learning

Will ensure that a formal review of filtering and monitoring systems takes place at least annually. This review will include recorded checks that filtering is operational on all internet-connected devices across all relevant locations, and will consider pupils who may be at greater risk of harm. Anglian Learning will ensure that filtering arrangements avoid unreasonable "over-blocking" which could restrict legitimate curriculum content or safeguarding education.

The Local Governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Safeguarding Governor will:

- Review the effectiveness of online safety systems and training.
- Ensure filtering and monitoring systems are appropriate and proportionate.
- Ensure leaders understand and manage filtering and monitoring systems effectively.

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 Local Governing Body for each Academy

The Governing Body will ensure that an annual online safety risk assessment is undertaken, reflecting emerging risks, pupil vulnerability profiles**,** filtering effectiveness, staff training needs and curriculum coverage.

3.3. The Designated Safeguarding Lead

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

- Ensuring that they can evidence that they have received appropriate training to ensure that they understand the risks associated with online safety, can recognise the additional risks learners with Special Educational Needs and Disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- Ensuring consistent implementation of this policy.
- Ensuring staff involved in monitoring or identifying online concerns are supported by senior leaders and are not expected to make safeguarding judgements independently.
- Working with the Headteacher, IT manager, or Director of ICT and other staff, as necessary, to address any online safety issues or incidents
- Where online activity gives rise to concern, the DSL will determine whether the matter constitutes a safeguarding concern and the appropriate response, including referral to children's social care, the police or other external agencies where required.
- Ensuring that any online safety incidents are recorded and managed in line with safeguarding procedures.
- Ensure that all staff receive appropriate online safety training
- Providing regular reports on online safety in school to the Headteacher and / or Local Governing Body
- Providing up-to-date information for parents routinely to ensure they are aware of emerging risks.
- Where generative AI tools are used within educational practice, the DSL and senior leaders will ensure safeguarding, data protection, ethical and filtering implications are risk assessed in line with DfE guidance on Generative AI in Education.

This list is not intended to be exhaustive.

3.4. Internet Filters and Monitoring in school:

Anglian Learning Trust ensure that there are systems in place for monitoring and filtering internet use. Filtering and monitoring systems are recognised as a safeguarding control and form part of the school's wider safeguarding systems. These systems are designed to help identify

potential safeguarding concerns, but do not replace professional judgement or staff vigilance**.**

The DSL team is responsible for:

- Ensuring that there is an annual, formal recorded review of the effectiveness of the filtering and monitoring systems in place.
- Considering who is 'potentially at greater risk of harm' and how they access the IT system.
- Reviewing concerns identified through the filtering and monitoring systems, determining safeguarding thresholds, and ensuring appropriate action is taken in line with the school's safeguarding procedures
- Monitoring data and trends regularly to inform safeguarding practice, training and curriculum planning.
- Ensuring that all staff understand filtering and monitoring arrangements, receive appropriate training.

Filtering and Educational opportunities

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request Technical Services to remove those sites from the filtered list for those pupils. Any requests to do so should be referred to the relevant Trust ICT Manager and clear reasons for the need must be established and recorded.
- Staff should be aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL (or a deputy) will consider a referral into the Cyber Choices programme. This programme aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

3.5. All staff and volunteers

All staff are expected to adhere to Anglian Learning's Code of Conduct**,** which sets out professional standards of behaviour, including expectations relating to the appropriate use of ICT, professional boundaries, and online conduct. Any concerns relating to staff behaviour online, including misuse of technology or breaches of professional standards, will be managed in accordance with the Code of Conduct and relevant disciplinary procedures.

All staff, including agency staff and other systems users, will agree and adhere to the terms laid out in the Anglian Learning ICT Policy, 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 policy and safeguarding policy.

This list is not intended to be exhaustive.

3.6. Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/ mobile/ connected devices in an appropriate way.

Parents are expected to:

- Keep their child safe online while at home and on any portable device by ensuring appropriate supervision and guidance is in place, including on those devices loaned by the school. Where a device is provided by a school, the school will ensure that it is set up with appropriate filters and monitoring software.
- Engage with guidance and information sharing events provided by the school to ensure parents are aware of emerging risks.
- Support the school by ensuring that their child understands and adheres to the pupil's acceptable use agreement

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships, Education, Relationships and Sex Education (RSE) and Health Education

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 and that support can be sought from trusted adults both in and outside school

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, and that this can be from trusted adults both inside and outside of school.

*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*
- *How to protect personal data and information online. e.g. through use of passwords.*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- *That some online content, images or profiles may be fake or digitally altered, including content generated using artificial intelligence, and that this can be misleading or harmful.*

All schools:

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

Online safety education is underpinned by the school's safeguarding procedures. Pupils are taught that some online behaviours and content may constitute abuse or exploitation and will be responded to through safeguarding processes as well as through behaviour systems.

Teaching will be adapted where appropriate for pupils with additional vulnerabilities, including SEND, communication needs, or social and emotional difficulties, recognising that some pupils may face increased online risk

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.

The school acknowledges that online risks continue to evolve, including the use of artificial intelligence to generate or manipulate content, online financial exploitation, sextortion and risks associated with livestreaming. Online safety education and safeguarding practice will be reviewed regularly to reflect emerging risks.

5. Cyber-bullying

5.1. 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's Positive Behaviour and Relationships and Anti-bullying Policy.)

5.2. 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.

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's Positive Behaviour and Relationships Policy and Safeguarding Policy. Where illegal, inappropriate or harmful material has been spread among pupils, a DSL must be made aware immediately. The school will use all reasonable endeavours to ensure the incident is contained involving external agencies for example Police and Social Care.

5.3. Examining electronic devices

School leaders 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, the DSL or other member of the senior leadership team will 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

6. Acceptable use of the internet in school

All pupils and staff, as part of the induction process, are expected to sign an agreement regarding the acceptable use of the academy's ICT systems.

Expectations relating to the use of social media, instant messaging platforms and electronic communication by staff are set out in Anglian Learning's Social Media and Instant Messaging Policy. This includes guidance on professional boundaries, appropriate communication with pupils, parents and colleagues, and the use of platforms such as messaging applications and online collaboration tools

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

Anglian Learning uses appropriate filtering and monitoring systems to safeguard users

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

7. Pupils using mobile devices in school

In line with DfE expectations, schools within Anglian Learning operate as mobile phone-free environments by default. Pupils do not have access to their mobile phones throughout the school day, including during lessons, transitions, breaktimes and lunchtimes, except in clearly defined and authorised exceptional circumstances. (See School's mobile phone and smart devices policy for further information about our approach)

8. How the school will respond to issues of misuse

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

Where the online behaviour of pupils involves harm, abuse, exploitation or risk of significant harm, incidents will be treated as safeguarding concerns and responded to through safeguarding procedures.

Staff misuse of ICT or online systems will be managed in accordance with the Code of Conduct and disciplinary procedures

Any staff related online sexual harassment, abuse and harmful sexual behaviour, including behaviour facilitated through digital platforms, is addressed within Anglian Learning's Sexual Harassment Policy**.** This policy sets out the Trust's approach to prevention, reporting, investigation and response, and should be read alongside this Online Safety Policy and the Safeguarding and Child Protection Policy.

9. Responding to online safety incidents

The following guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities;

- Where online activity gives rise to safeguarding concerns, including abuse, exploitation or risk of significant harm, responses will be managed in line with Anglian Learning's Safeguarding and Child Protection Policy**,** rather than solely through behaviour procedures.
- When responding to online safety incidents, the school will take steps to ensure that evidence is preserved and recorded appropriately. Serious or harmful incidents will be escalated in line with safeguarding procedures.
- Decisions about escalation, including referral to the police or CEOP, will be made by the DSL or senior safeguarding lead. Records of incidents and actions taken will be maintained as part of the school's safeguarding record
- Detailed procedures relating to incidents involving the sharing of nude or semi-nude images are set out in the Safeguarding and Child Protection Policy and UKCIS guidance.
- This guidance does not apply to adults sharing nudes or semi-nudes of under 18-year-olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.
- **If an incident comes to your attention report it to the DSL immediately.**

Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**. Please refer to the DSL, the safeguarding procedures and the UKCIS guidance for further information and advice.

The DSL will refer to safeguarding policies, KCSIE and other guidance to consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

The school is committed to providing annual and ongoing training to ensure that:

- Staff are aware of online safeguarding issues including cyber-bullying and grooming and how to respond to these
- Staff are aware of emerging risks
- Staff are equipped to deliver the e-safety curriculum
- Staff are knowledgeable about their responsibilities regarding filtering and monitoring systems and their purpose as well as how to escalate concerns
- All new staff members will receive online safety training, as part of their induction process.

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

11. Remote Education

Where remote education is delivered, safeguarding arrangements mirror in-school expectations. This includes appropriate filtering, staff conduct standards, supervision, clear identification of approved platforms, and communication with parents regarding online interactions and expectations.

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Positive Behaviour and Relationships policy
- Staff disciplinary procedures
- Data Protection Policy and Privacy Notices
- Complaints procedure
- ICT and internet acceptable use policy
- Mobile phone and Smart Devices policy
- Sexual Harassment Policy
- Social Media and Instant Messaging Policy
- Code of conduct

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents / carers)

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

When I use the academy's ICT systems (e.g. 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, or trusted adult 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 schoolwork 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.	

Signed (pupil):	**Date:**
Parent / Carer agreement: I agree that my child can use the academy'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 academy'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 2: KS2 acceptable use agreement (pupils and parents / carers)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the academy's ICT systems (e.g. computers) and get onto the internet in school I will:** • Always use the academy's ICT systems and the internet responsibly and for educational purposes only • Only use them when a member of staff 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 member of staff in school 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 • Open any attachments in emails, or follow any links in emails, without first checking with an adult. • Use any inappropriate language when communicating online, including in emails • Log in to the academy'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 devices (including smart watches) into school:** • I will hand it into the front office at the beginning of the day for safe keeping and then collect it at the end of the school day. I will not use it at clubs, other activities organised by the school or bring it on school trips. **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:**

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?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are you aware of which groups of pupils may have additional vulnerabilities when online?	
Was E Safety and filtering and monitoring referred to in your induction process?	
Are there any areas of online safety in which you would like training / further training?	