ANGLIAN LEARNING

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

ONLINE SAFETY POLICY

THIS POLICY WAS APPROVED:	AUTUMN 2023
POLICY VERSION:	2.0
THIS POLICY WILL BE REVIEWED:	AUTUMN 2025
MEMBER OF STAFF WITH RESPONSIBILITY FOR REVIEW:	DIRECTOR OF INCLUSION
THIS POLICY WAS CONSULTED WITH:	DESIGNATED SAFEGUARDING LEADS 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

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2023, 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/).

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 Behaviour 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. The Local Governing Body for each Academy

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

The Safeguarding Governor regularly reviews the effectiveness of online safety systems and training requirements. This includes the filtering and monitoring systems in place.

The Safeguarding Governor seeks to ensure that the leadership team and staff have an awareness of and understanding of the filters and monitoring provisions in place, that they are managed effectively and know how to escalate concerns when identified.

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 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 that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Headteacher, ICT Team Leader, incumbent third party support provider or Director of ICT and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents including Cyber Bullying are logged using MyConcern and dealt with appropriately in line with the Safeguarding Policy and Behaviour Policy
- Ensure that all staff receive online safety training as part of their child protection training at induction. This should include amongst other things, an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. (appendix 3 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 Local Governing Body
- Providing up-to-date information for parents routinely to ensure they are aware of emerging risks.

This list is not intended to be exhaustive.

3.3. Internet Filters and Monitoring in school:

Anglian Learning Trust ensure that there are systems in place for monitoring and filtering internet use.

The DSL team is responsible for:

- Ensuring that there are regular reviews 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.

Ensuring that all staff

- Understand their roles and responsibilities in relation to filtering and monitoring.
- Receive regular (at least annually) online safety training and updates including understanding the filtering and monitoring systems and processes in place.
- Use these filtering, monitoring and protection systems, which are updated on a regular basis to keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and that they know how to escalate concerns when identified

- Ensure 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.

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 IT support to remove those sites from the filtered list for those pupils. Any requests to do so should be audited by the IT Network Manager/ DSL, 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.

3.4. All staff and volunteers

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.

3.5. 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 pupils acceptable use policy.

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

Academies that do not follow the National Curriculum should adapt this section to include details of how online safety forms part of their own curriculum.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Primary Schools:

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*
- *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*

Secondary schools:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, understand the associated risks and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*

- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

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

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

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 academy Behaviour 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 academy Behaviour 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 the 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.

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.

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 the Anglian Learning ICT Policy and appendices 1, 2 and 3.

7. Pupils using mobile devices in school

Pupils may bring mobile devices into school. Phones must be turned off and handed into the school office for the school day. They are only to be turned on at the end of the day and when leaving the school site.

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.

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 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 / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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;

- Advice for schools on how to respond to the sharing of "nudes and semi-nudes" (formerly referred to as 'sexting' and 'youth produced sexual imagery') is in the School's Safeguarding and Protecting Children Policy and Procedures.
- The latest advice from UKCIS (December 2020) defines this activity as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.
- The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.
- 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.

9. 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.
- 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
- 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.

10. 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

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 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?	