eat.uk.com
@EthosAcadTrust

Company Registration Number: 10745840 (England and Wales)

Ethos Academy Trust

Online Safety Policy

October 2025

ETHOS ACADEMY TRUST

Nurturing inclusive learning communities

1	**Summary**	Online Safety
2	**Responsible person**	Headteacher / Head of School
3	**Accountable ELT member**	Rebecca Smith
4	**Applies to**	☒All Staff ☐Support Staff ☐Teaching Staff
5	**Trustees and/or individuals who have overseen development of this policy**	Rebecca Smith
6	**Headteachers/Service Heads who were consulted and have given approval (if applicable)**	
8	**Ratifying committee(s) and date of final approval**	Learning and Achievement Committee 03.11.25 via email
9	**Version number**	1.7
10	**Available on**	Every ☒Y ☐N Trust Website ☒Y☐N Academy Website ☒Y☐N Staff Portal ☐Y☒N
11	**Related documents (if applicable)**	Safeguarding and Child Protection
12	**Disseminated to**	☐Trustees ☒All Staff ☐Support Staff ☐Teaching Staff
13	**Date of implementation (when shared)**	October 2025
14	**Date of next formal review**	October 2026
15	**Consulted with Recognised Trade Unions**	☐Y ☒N

Date	Version	Action	Summary of changes
October 2025	1.7	Major policy revision	Re-write of original documentation

Contents

Section	Description	Page
1	Aims	3
2	Legislation and guidance	3
3	Roles and responsibilities	3
4	Education about online safety	7
5	Remote Learning Safety	7
6	Cyber-bullying	8
7	Acceptable use of the internet in schools	10
8	Staff using work devices outside of the schools	10
9	How the schools will respond to issues of misuse	11
10	Training	11

1. Aims

Ethos Academy Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 (RSE) and health 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Ethos Academy Trust.

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the Executive Team (and through them the Heads) to account for its implementation. The Board will review

effectiveness by receiving regular information about online safety incidents and monitoring reports from The Trust Safeguarding and Inclusion Lead.

All Trustees 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

The Board will ensure that appropriate filtering and monitoring systems are in place, whilst being careful that the system does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

3.2 The Headteacher / Head of School

The Headteacher / Head of School is responsible for:

- Making sure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT provider to make sure the appropriate systems and processes are in place
- Providing Trustees with assurance that filtering and monitoring systems are working effectively and are reviewed regularly

3.3 The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety in the individual schools, in particular:

- Supporting the Headteacher / Head of School in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Headteacher / Head of School, ICT provider 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The ICT Provider

The ICT provider is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy and have read, understood and signed the Acceptable Use Agreement
- Implementing this policy consistently
- Ensuring that pupils understand and follow the Online Safety Policy guidelines as appropriate.
- Reporting any suspected misuse or problem to the Head or DSL
- 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 relevant school's behaviour policy
- Ensuring that all digital communications, particularly with pupils and/or parents/carers are on a professional level and be made using EAT email addresses. Staff should not use personal email addresses for official communications
- Ensuring that online safety issues are embedded in all aspects of the curriculum and other activities

- Monitoring the use of digital technologies, mobile devices, cameras and similar devices in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Ensuring that whenever the internet is used, pupils are guided to sites suitable for their use and that processes are in place for dealing with any unsuitable material from internet searches.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet along with mobile and similar devices in an appropriate way. The Trust will take every opportunity to help parents and carers understand these issues through parents' events, newsletters, letters and websites.

Parents and carers will be encouraged to support the Trust in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website, learning platforms and online pupil records.
- Their children's personal devices in the school, where this is allowed.

Parents are expected to:

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

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

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 Pupils

Pupils will be expected and supported to:
• Use the Trust's digital technology systems in accordance with the Pupil Acceptable Use Agreement which they should sign; where appropriate it would be expected that parents or carers would sign on behalf of the pupils.
• Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• Understand the importance of adopting good online safety practice when using digital technologies out of school
• Know what action to take if they or someone they know feels worried or vulnerable when using online technology.

3.8 Visitors and contactors

Visitors and members of the community who use the Trust'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.

4. Education about online safety

4.1 Pupils

Pupils will be taught about online safety as part of the PSHE curriculum. Details of the individual's school's curriculum can be found on their website.

4.2 Parents/carers

The schools will raise parents/carers' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

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

5. Remote Learning Safety

To protect students and staff during online education:

- Only school-approved platforms may be used for remote learning.
- Video conferencing should be conducted professionally, with privacy and appropriate behaviour maintained.
- Students must show respectful conduct and avoid sharing personal or login information.
- Staff must safeguard sensitive data and ensure all communication is learning-focused.
- Any safeguarding concerns during remote sessions must be reported to the Designated Safeguarding Lead.

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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 encourage them to do so, including where they are a witness rather than the victim.

The schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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 receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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 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.

6.3 Examining electronic devices

The Head, and any member of staff authorised to do so by the Head, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Senior Leadership Team.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team 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.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Ethos Academy Trust recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Ethos Academy Trust will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and Trustees 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 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 and restrict access through filtering systems where appropriate.

8. Staff using work devices outside of 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
- Ensuring that hard drives and USB's are not used for storing work information
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school'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 Trust ICT provider.

8. How the schools will respond to issues of misuse

Where a pupil misuses the school's ICT systems or the internet, we will follow the procedures set out in our policies. 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 code of conduct and staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

9. Training

All new staff members will receive training 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:

- 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, threatening, 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 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 will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Trustees 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.